ESET Smart Security

Integrated components:
ESET NOD32 Antivirus
ESET NOD32 Antispyware
ESET Personal Firewall
ESET Antispam

New generation of NOD32 technology

User Guide

we protect your digital worlds

contents

1. ESET Smart Security 4
1.1 What's new 4
1.2 System requirements 4

2. Installation 5
2.1 Typical installation 5
2.2 Custom installation 6
2.3 Using original settings 8
2.4 Entering User name and password 8
2.5 On-demand computer scan 8

3. Beginner's guide 9
3.1 Introducing user interface design – modes 9
3.1.1 Checking operation of the system 9
3.1.2 What to do if the program doesn't work properly ... 10
3.2 Update setup 10
3.3 Trusted zone setup 10
3.4 Proxy server setup 11
3.5 Settings protection 11

4. Work with ESET Smart Security 12
4.1 Antivirus protection 12
4.1.1 Real-time file system protection 12
4.1.1.1 Control setup 12
4.1.1.1.1 Media to scan 12
4.1.1.1.2 Scan on (Event-triggered scanning) 12
4.1.1.1.3 Additional ThreatSense parameters for newly created files 12
4.1.1.1.4 Advanced setup 12
4.1.1.2 Cleaning levels 12
4.1.1.3 When to modify the real-time protection configuration 13
4.1.1.4 Checking real-time protection 13
4.1.1.5 What to do if the real-time protection does not work 13
4.1.2 Email protection 13
4.1.2.1 POP3 checking 13
4.1.2.1.1 Compatibility 13
4.1.2.2 Integration with Microsoft Outlook, Outlook Express, and Windows Mail 14
4.1.2.2.1 Appending tag messages to email body 14
4.1.2.3 Removing infiltrations 14
4.1.3 Web access protection 14
4.1.3.1 HTTP 14
4.1.3.1.1 Blocked / excluded addresses 15
4.1.3.1.2 Web browsers 15
4.1.4 Computer scan 15
4.1.4.1 Type of scan 16
4.1.4.1.1 Standard scan 16
4.1.4.1.2 Custom scan 16
4.1.4.2 Scan targets 16
4.1.4.3 Scan profiles 16
4.1.5 ThreatSense engine parameters setup 16
4.1.5.1 Objects setup 17
4.1.5.2 Options 17
4.1.5.3 Cleaning 18
4.1.5.4 Extensions 18
4.1.6 An infiltration is detected 18
4.2 Personal firewall 19
4.2.1 Filtering modes 19
4.2.2 Block all traffic: disconnect network 19
4.2.3 Disable filtering: allow all traffic 19
4.2.4 Configuring and using rules 19
4.2.4.1 Creating new rules 20
4.2.4.2 Editing rules 20
4.2.5 Configuring zones 20
4.2.6 Establishing connection – detection 20
4.2.7 Logging 21

ESET Smart Security

Copyright © 2007 by ESET, spol. s r. o.

ESET Smart Security was developed by ESET, spol. s r.o.
For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without a permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Customer Care Worldwide: www.eset.com/support
Customer Care for Europe: www.eset.eu/support

REV.20071129-003

4.3 Antispam protection 21
4.3.1 Self-learning Antispam 22
4.3.1.1 Adding addresses to whitelist 22
4.3.1.2 Marking messages as spam 22
4.4 Updating the program 22
4.4.1 Update setup 22
4.4.1.1 Update profiles 23
4.4.1.2 Advanced update setup 23
4.4.1.2.1 Update mode 23
4.4.1.2.2 Proxy server 24
4.4.1.2.3 Connecting to LAN 24
4.4.1.2.4 Creating update copies – Mirror 24
4.4.1.2.4.1 Updating from the Mirror 25
4.4.1.2.4.2 Troubleshooting Mirror update problems 26
4.4.2 How to create update tasks 26
4.5 Scheduler 26
4.5.1 Purpose of scheduling tasks 26
4.5.2 Creating new tasks 27
4.6 Quarantine 27
4.6.1 Quarantining files 27
4.6.2 Restoring from Quarantine 27
4.6.3 Submitting file from Quarantine 27
4.7 Log files 28
4.7.1 Log maintenance 28
4.8 User interface 28
4.8.1 Alerts and notifications 29
4.9 ThreatSense.Net 29
4.9.1 Suspicious files 30
4.9.2 Statistics 30
4.9.3 Submission 31
4.10 Remote administration 31
4.11 License 32

5. Advanced user 33

5.1 Proxy server setup 33
5.2 Export / import settings 33
5.2.1 Export settings 33
5.2.2 Import settings 33
5.3 Command Line 33

6. Glossary 35

6.1 Types of infiltrations 35
6.1.1 Viruses 35
6.1.2 Worms 35
6.1.3 Trojan horses 35
6.1.4 Rootkits 35
6.1.5 Adware 35
6.1.6 Spyware 36
6.1.7 Potentially unsafe applications 36
6.1.8 Potentially unwanted applications 36
6.2 Types of remote attacks 36
6.2.1 DoS attacks 36
6.2.2 DNS Poisoning 36
6.2.3 Worm attacks 36
6.2.4 Port scanning 36
6.2.5 TCP desynchronization 36
6.2.6 SMB Relay 37
6.2.7 ICMP attacks 37
6.3 E-mail 37
6.3.1 Advertisements 37
6.3.2 Hoaxes 37
6.3.3 Phishing 37
6.3.4 Recognizing spam scams 38
6.3.4.1 Rules 38
6.3.4.1 Bayesian filter 38
6.3.4.2 Whitelist 38
6.3.4.3 Blacklist 38
6.3.4.5 The server-side control 38

1. ESET Smart Security

ESET Smart Security is the first representative of the new approach to truly integrated computer security. It utilizes the speed and precision of ESET NOD32 Antivirus, which is guaranteed by the most recent version of the ThreatSense® scanning engine, combined with the tailor-made Personal firewall and Antispam modules. The result is an intelligent system which is constantly on alert for attacks and malicious software endangering your computer.

ESET Smart Security is not a clumsy conglomerate of various products in one package, as offered by other vendors. It is the result of a long-term effort to combine maximum protection with minimum system footprint. The advanced technologies based on artificial intelligence are capable of proactively eliminating the penetration of viruses, spyware, trojan horses, worms, adware, rootkits, and other Internet-borne attacks without hindering system performance or disrupting your computer.

1.1 What's new

The long-time development experience of our experts is demonstrated by the entirely new architecture of the ESET Smart Security program, which guarantees maximum detection with minimum system requirements. The complex security solution contains modules with several advanced options. The following list offers you a brief overview of these modules.

Antivirus & antispyware

This module is built upon the ThreatSense® scanning core, which was used for the first time in the award-winning NOD 32 Antivirus system. The ThreatSense® core is optimized and improved with the new ESET Smart Security architecture.

Feature	Description
Improved Cleaning	The antivirus system now intelligently cleans and deletes most of the detected infiltrations without requiring user intervention.
Background Scanning Mode	Computer scanning can be launched in the background without slowing down performance.
Smaller Update Files	Core optimization processes keep the size of update files smaller than in version 2.7. Also, the protection of update files against damage has been improved.
Popular EMail Client Protection	It is now possible to scan incoming mail not only in MS Outlook but also in Outlook Express and Windows Mail.
Variety of Other Minor Improvements	– Direct access to file systems for high speed and throughput. – Blocking access to infected files – Optimization for the Windows Security Center, including Vista.

Personal firewall

The Personal firewall monitors all traffic between a protected computer and other computers in the network. ESET Personal firewall contains advanced functions as listed below.

Feature	Description
Low layer network communication scanning	Network communication scanning on the Data Link Layer enables ESET Personal firewall to overcome a variety of attacks that would otherwise be undetectable.
IPv6 support	ESET Personal firewall displays IPv6 addresses and allows users to create rules for them.
Executable file monitoring	Monitoring changes in executable files in order to overcome infection. It is possible to allow file modification of signed applications.
File scanning integrated with HTTP and POP3	Integrated file scanning into the HTTP and POP3 application protocols. Users are protected when browsing the Internet or downloading emails.
Intrusion Detection System	Ability to recognize the character of network communication and various types of network attacks and an option to automatically ban such communication.
Interactive, Automatic or Policy-based mode support	Users can select whether the firewall actions will be executed automatically, or if they want to set rules interactively. Communication in policy-based mode is handled according to rules predefined by the user or the network administrator.
Supersedes Integrated Windows Firewall	Supersedes the Integrated Windows Firewall, it also interacts with the Windows Security Center so the user is always informed about his security status. ESET Smart Security installation turns off the windows firewall by default

Antispam

ESET Antispam filters unsolicited email and therefore increases the security and comfort of electronic communication.

Feature	Description
Incoming Mail Scoring	All Incoming mail is assigned a rating ranging from 0 (a message is not spam) to 100 (a message is spam), and transferred accordingly into the Junk Mail folder or into a custom folder created by the user. Parallel scanning of incoming emails is possible.
Supports a variety of scanning techniques	– Bayes analysis – Rule-based scanning – Global fingerprint database check
Full integration with email clients	Antispam protection is available to users of Microsoft Outlook, Outlook Express and Windows Mail clients.
Manual spam selection is available	There is an option to manually check / uncheck email as spam.

1.2 System requirements

For seamless operation of ESET Smart Security and ESET Smart Security Business Edition, the system should meet the following hardware and software requirements:

ESET Smart Security:

Windows 2000, XP	400 MHz 32-bit / 64-bit (x86 / x64) 128 MB RAM of system memory 35 MB available space Super VGA (800 × 600)
Windows Vista	1 GHz 32-bit / 64-bit (x86 / x64) 512 MB RAM of system memory 35 MB available space Super VGA (800 × 600)

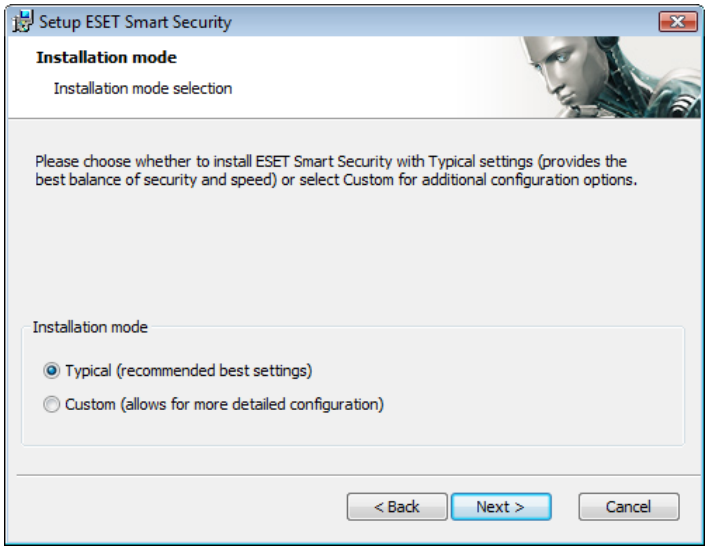
ESET Smart Security Business Edition:

Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32-bit / 64-bit (x86 / x64) 128 MB RAM of system memory 35 MB available space Super VGA (800 × 600)
Windows Vista	1 GHz 32-bit / 64-bit (x86 / x64) 512 MB RAM of system memory 35 MB available space Super VGA (800 × 600)

2. Installation

After purchase, the ESET Smart Security installer can be downloaded from ESET's web site. It comes as an ess_nt**_***.msi (ESET Smart Security) or essbe_nt**_***.msi (ESET Smart Security Business Edition) package. Launch the installer and the installation wizard will guide you through the basic setup. There are two types of installation available with different levels of setup details:

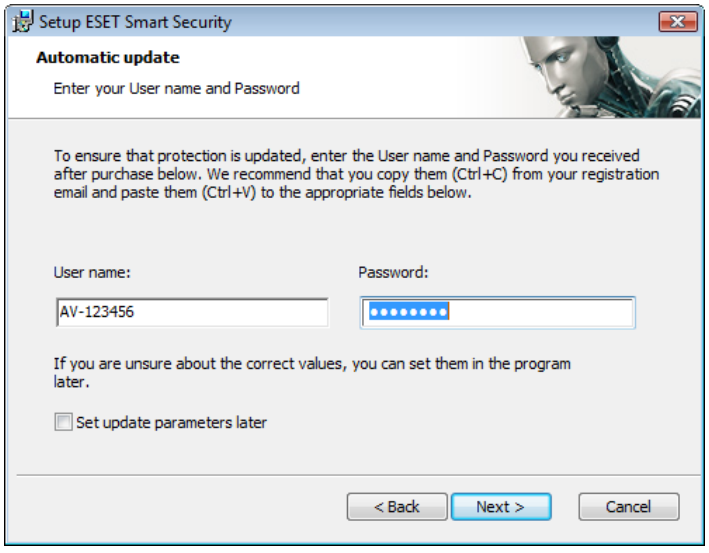
1. Typical installation
2. Custom installation


Setup ESET Smart Security
Installation mode
Installation mode selection
Please choose whether to install ESET Smart Security with Typical settings (provides the best balance of security and speed) or select Custom for additional configuration options.
Installation mode
Typical (recommended best settings)
Custom (allows for more detailed configuration)
< Back
Next >
Cancel

2.1 Typical installation

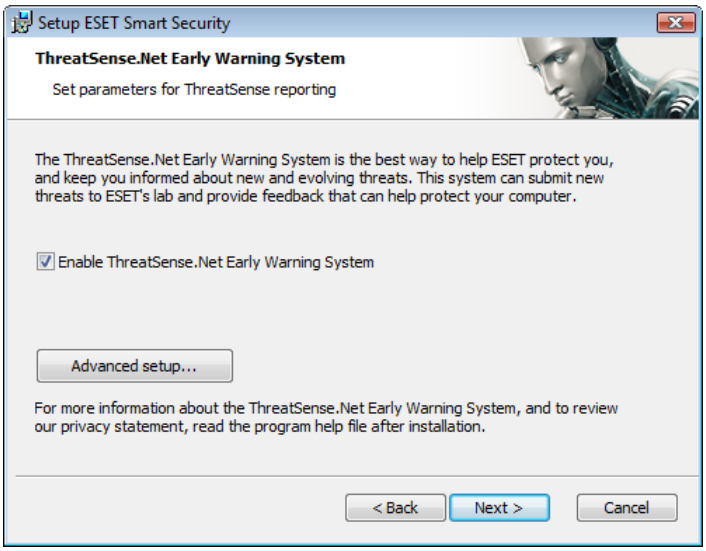
The Typical installation is recommended for users who want to install ESET Smart Security with the default settings. The default settings of the program provide the maximum level of protection, a fact appreciated by those users who do not want to configure detailed settings.

The first (very important) step is to enter the user name and password for automatic updating of the program. This plays a significant role in providing constant protection of the system.


Setup ESET Smart Security
Automatic update
Enter your User name and Password
To ensure that protection is updated, enter the User name and Password you received after purchase below. We recommend that you copy them (Ctrl+C) from your registration email and paste them (Ctrl+V) to the appropriate fields below.
User name:
Password:
AV-123456
If you are unsure about the correct values, you can set them in the program later.
Set update parameters later
< Back
Next >
Cancel

Enter your **User name** and **Password**, i.e. the authentication data you received after the purchase or registration of the product, into the corresponding fields. If you do not currently have your User name and Password available, select the **Set update parameters later** option. Authentication data can be inserted at any time later on, directly from the program.

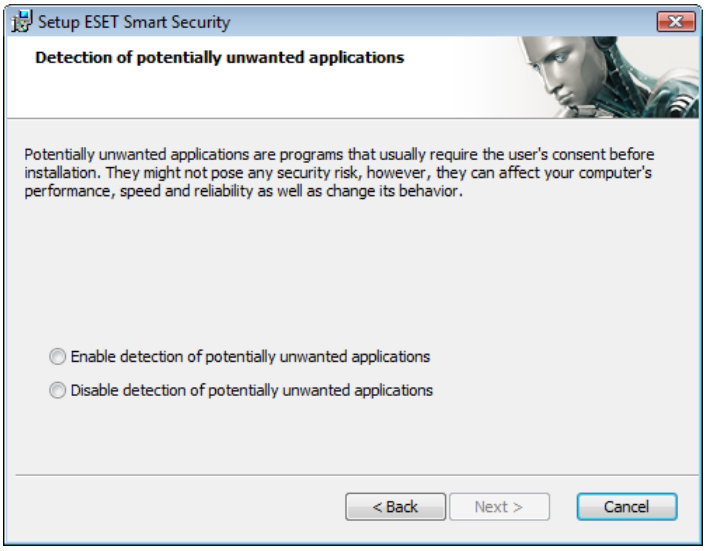
The next step in the installation is configuration of the ThreatSense.Net Early Warning System. The ThreatSense.Net Early Warning System helps to ensure that ESET is immediately and continuously informed about new infiltrations in order to quickly protect its customers. The system allows for submission of new threats to ESET's virus laboratory, where they are analyzed, processed and added to the virus signature databases.


Setup ESET Smart Security
ThreatSense.Net Early Warning System
Set parameters for ThreatSense reporting
The ThreatSense.Net Early Warning System is the best way to help ESET protect you, and keep you informed about new and evolving threats. This system can submit new threats to ESET's lab and provide feedback that can help protect your computer.
Enable ThreatSense.Net Early Warning System
Advanced setup...
For more information about the ThreatSense.Net Early Warning System, and to review our privacy statement, read the program help file after installation.
< Back
Next >
Cancel

By default, the **Enable ThreatSense.Net Early Warning System** check box is selected, which will activate this feature. Click **Advanced setup...** to modify detailed settings for the submission of suspicious files.

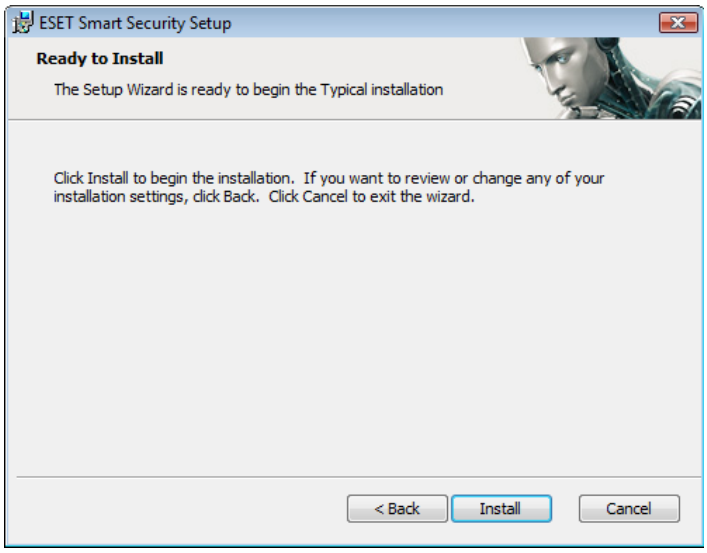
The next step in the installation process is to configure the **Detection of potentially unwanted applications**. Potentially unwanted applications are not necessarily intended to be malicious, but can often negatively affect the behavior of the operating system.

These applications are often bundled with other programs and may be difficult to notice during the installation process. Although these applications usually display a notification during installation, they can easily be installed without your consent.


Setup ESET Smart Security
Detection of potentially unwanted applications
Potentially unwanted applications are programs that usually require the user's consent before installation. They might not pose any security risk, however, they can affect your computer's performance, speed and reliability as well as change its behavior.
Enable detection of potentially unwanted applications
Disable detection of potentially unwanted applications
< Back
Next >
Cancel

Select the **Enable detection of potentially unwanted applications** option to allow ESET Smart Security to detect this type of threat (recommended).

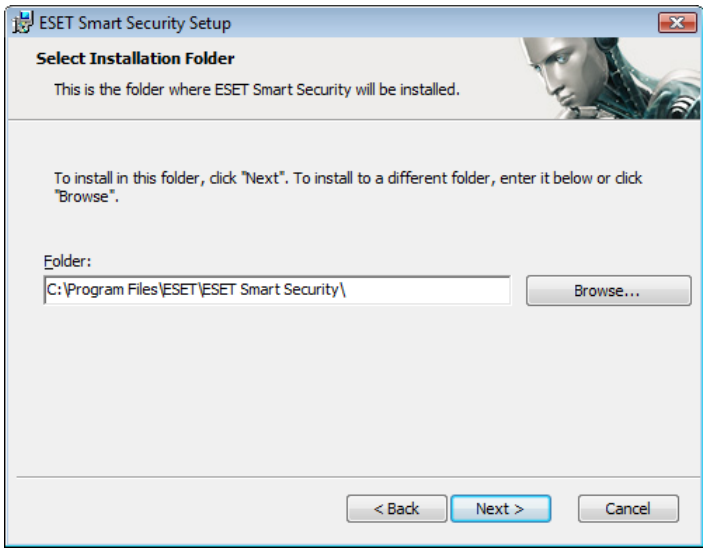
The last step in the Typical installation mode is confirmation of the installation by clicking the **Install** button.


ESET Smart Security Setup
Ready to Install
The Setup Wizard is ready to begin the Typical installation
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
< Back
Install
Cancel

2.2 Custom installation

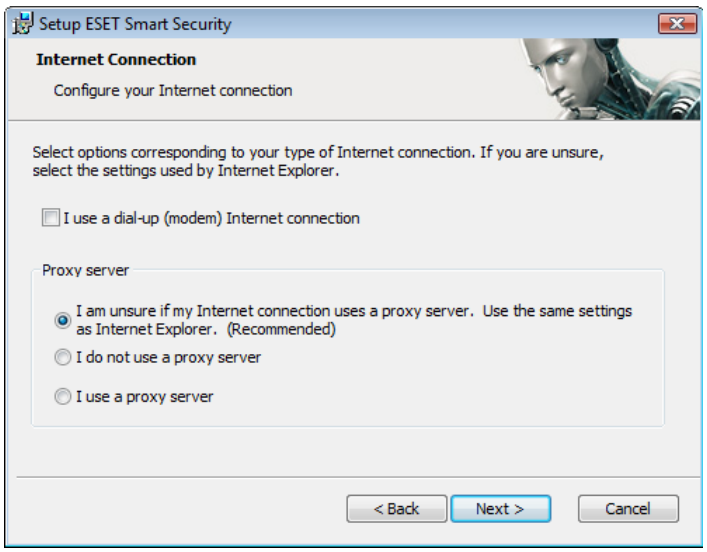
The **Custom** installation is designed for users who have experience with fine-tuning programs and who wish to modify advanced settings during installation.

The first step is to select the destination location for the install. By default, the program installs into C:\Program Files\ESET\ESET Smart Security\. Click **Browse...** to change this location (not recommended).

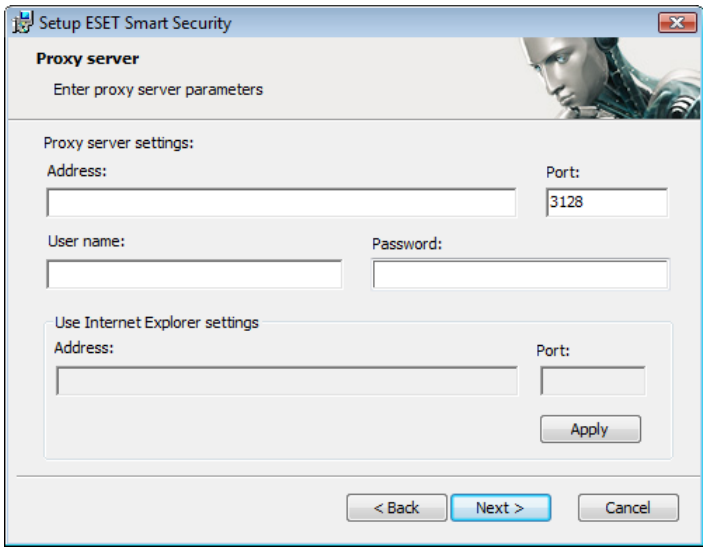

ESET Smart Security Setup
Select Installation Folder
This is the folder where ESET Smart Security will be installed.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\ESET\ESET Smart Security\
Browse...
< Back
Next >
Cancel

Next, **Enter your User name and Password**. This step is the same as in the Typical installation (see page 5).

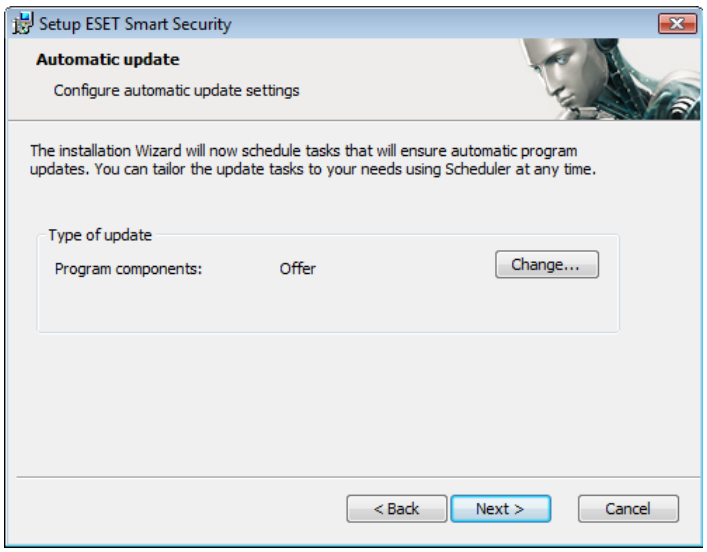
After entering your User name and Password, click **Next** to **Configure your Internet connection**.


Setup ESET Smart Security
Internet Connection
Configure your Internet connection
Select options corresponding to your type of Internet connection. If you are unsure, select the settings used by Internet Explorer.
I use a dial-up (modem) Internet connection
Proxy server
I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer. (Recommended)
I do not use a proxy server
I use a proxy server
< Back
Next >
Cancel

If you use a proxy server, it must be correctly configured in order for virus signature updates to work properly. If you don't know whether you use a proxy server to connect to the Internet, leave the default setting **I am unsure if my Internet connection uses a proxy server. Use the same settings as Internet Explorer** and click **Next**. If you do not use a proxy server, select the corresponding option.

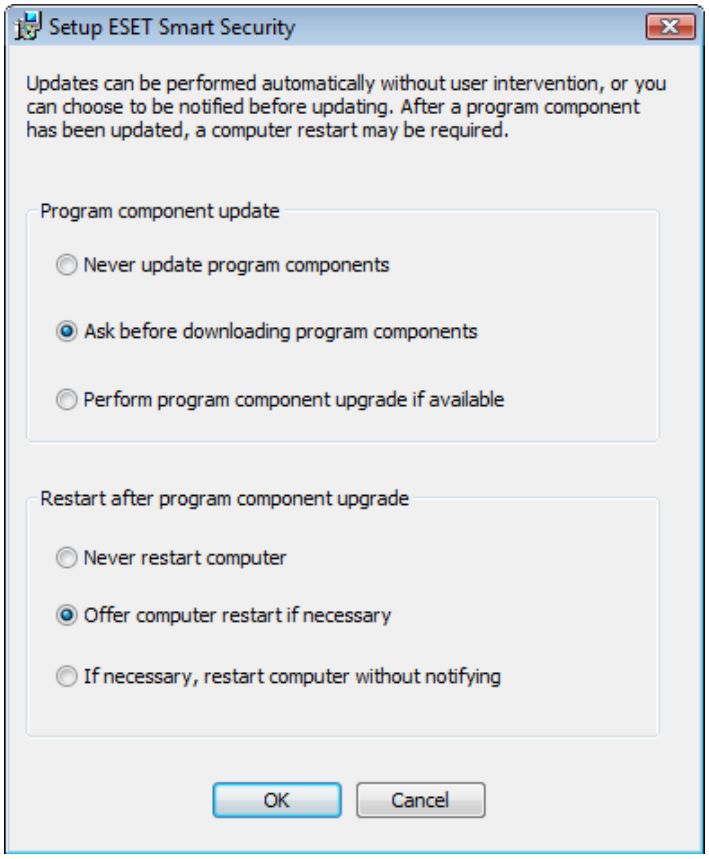


To configure your proxy server settings, select **I use a proxy server** and click **Next**. Enter the IP address or URL of your proxy server in the **Address field.** In the **Port** field, specify the port where the proxy server accepts connections (3128 by default). In the event that the proxy server requires authentication, a valid user name and password must be entered, granting access to the proxy server. Proxy server settings can also be copied from Internet Explorer if desired. To do this, click **Apply** and confirm the selection.


Setup ESET Smart Security
Automatic update
Configure automatic update settings
The installation Wizard will now schedule tasks that will ensure automatic program updates. You can tailor the update tasks to your needs using Scheduler at any time.
Type of update
Program components:
Offer
Change...
< Back
Next >
Cancel

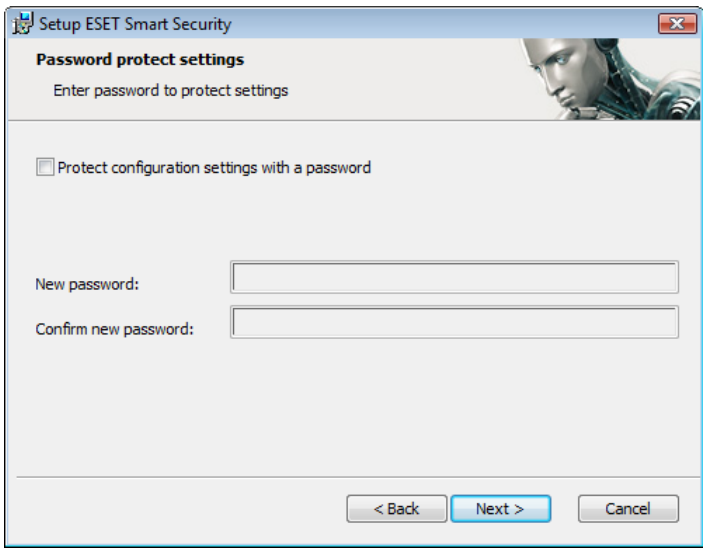
Click **Next** to proceed to the **Configure automatic update settings** window. This step allows you to designate how automatic program component updates are to be handled on your system. Click **Change...** to access the advanced settings.

If you do not want program components to be updated, select **Never update program components**. Enabling the **Ask before downloading program components** option will display a confirmation window before downloading program components. To enable automatic program component upgrades without prompting, select the option **Perform program component upgrade if available**.


Setup ESET Smart Security
Updates can be performed automatically without user intervention, or you can choose to be notified before updating. After a program component has been updated, a computer restart may be required.
Program component update
Never update program components
Ask before downloading program components
Perform program component upgrade if available
Restart after program component upgrade
Never restart computer
Offer computer restart if necessary
If necessary, restart computer without notifying
OK
Cancel

NOTE: After a program component upgrade, a reboot is usually required. The recommended setting is: **If necessary, restart computer without notifying**.

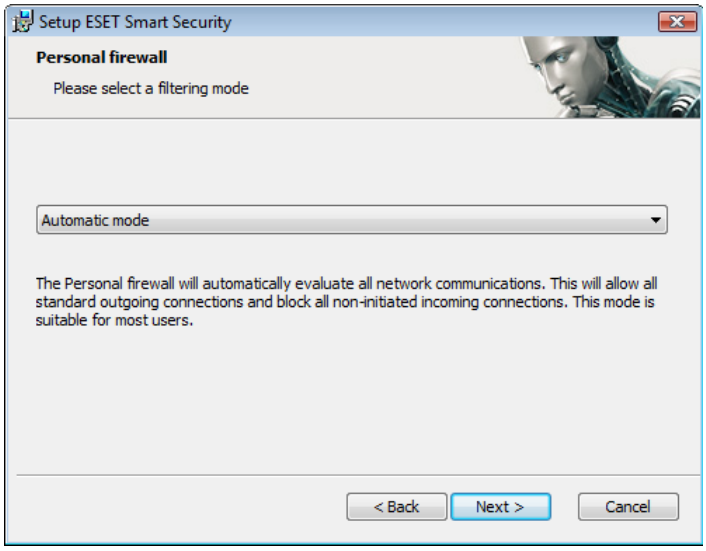
The next step in the installation is to Enter a password to protect program parameters. Choose a password you wish to protect the program with. Retype the password to confirm.



The steps **Configuration of the ThreatSense.Net Early Warning System** and **Detection of potentially unwanted applications** are the same as for a Typical installation, and are not shown here (see page 5).

The last step in Custom mode is to select the ESET Personal firewall filtering mode. Three modes are available:

- **Automatic**
- **Interactive**
- **Policy-based**


Setup ESET Smart Security
Personal firewall
Please select a filtering mode
Automatic mode
The Personal firewall will automatically evaluate all network communications. This will allow all standard outgoing connections and block all non-initiated incoming connections. This mode is suitable for most users.
< Back
Next >
Cancel

Automatic mode is recommended for the majority of users. All standard outgoing connections are enabled (automatically analyzed using predefined settings) and unsolicited incoming connections are automatically blocked.

Interactive mode is suitable for advanced users. Communications are handled by user-defined rules. If there is no rule defined for a communication, the program asks the user to allow or deny the communication.

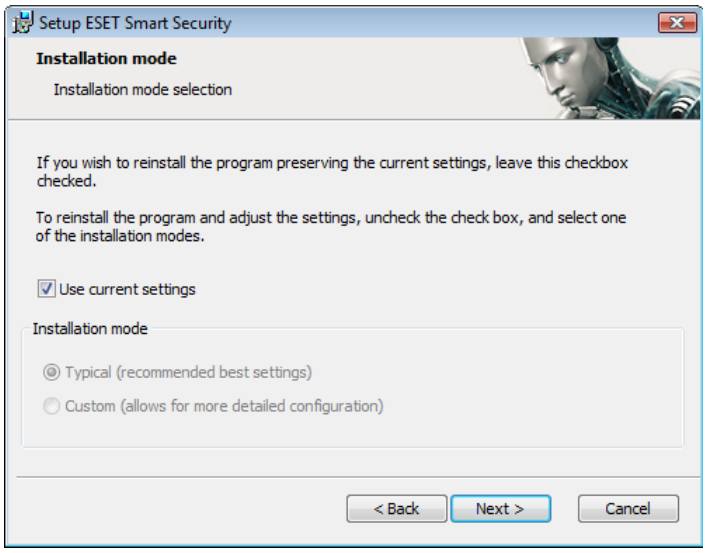
Policy-based mode evaluates communications based on predefined rules created by the administrator. If there is no rule available, the connection is automatically blocked and the user sees no warning

message. We recommend that you only select the policy-based mode if you are an administrator who intends to configure network communication.

The last step shows a window requiring your consent to install.

2.3 Using original settings

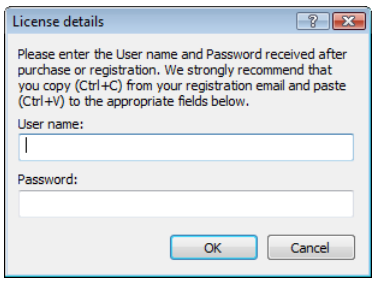
If you reinstall ESET Smart Security, the **Use current settings** option is displayed. Select this option to transfer setup parameters from the original installation to the new one.


Setup ESET Smart Security
Installation mode
Installation mode selection
If you wish to reinstall the program preserving the current settings, leave this checkbox checked.
To reinstall the program and adjust the settings, uncheck the check box, and select one of the installation modes.
Use current settings
Installation mode
Typical (recommended best settings)
Custom (allows for more detailed configuration)
< Back
Next >
Cancel

2.4 Entering User name and password

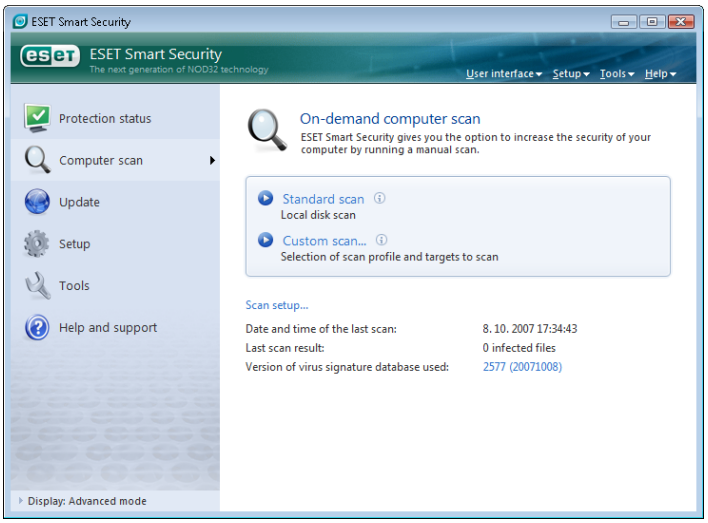
For optimal functionality, it is important that the program is automatically updated. This is only possible if the correct user name and password are entered in the update setup.

If you did not enter your user name and password during the installation, you can do so now. In the main program window, click **Update** and then click **User name and Password Setup...** Enter the data you received with your product license into the **License details** window.


License details
Please enter the User name and Password received after purchase or registration. We strongly recommend that you copy (Ctrl+C) from your registration email and paste (Ctrl+V) to the appropriate fields below.
User name:
Password:
OK
Cancel

2.5 On-demand computer scan

After installation of ESET Smart Security, a computer scan for the presence of malicious code should be performed. To quickly launch a scan, select **Computer scan** from the main menu and then select **Standard scan** in the main program window. For more information about the Computer scan feature, see the chapter "Computer scan".



3. Beginner's guide

This chapter provides an initial overview of ESET Smart Security and its basic settings.

3.1 Introducing user interface design – modes

The main window of ESET Smart Security is divided into two main sections. The left column provides access to the user-friendly main menu. The main program window on the right predominantly serves to display information corresponding to the option selected in the main menu.

The following is a description of buttons within the main menu:

Protection status – In a user-friendly form, it provides information about the protection status of ESET Smart Security. If the Advanced mode is activated, the status of all protection modules is displayed. Click on a module to view its current status.

Computer scan – This option allows the user to configure and launch the On-demand computer scan.

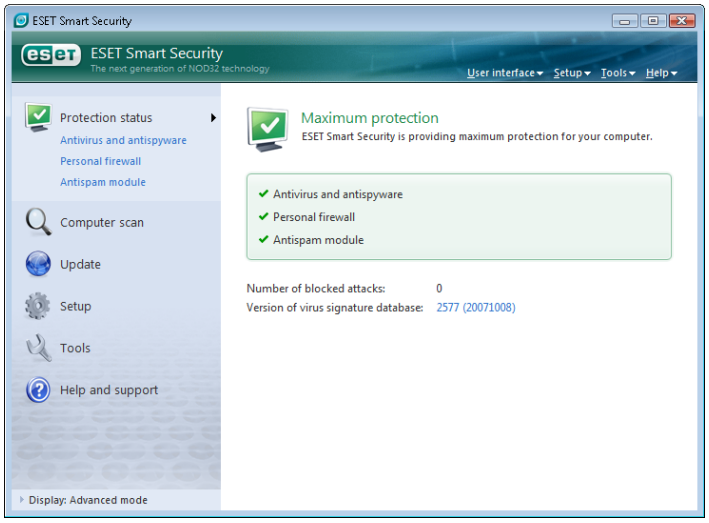
Update – Select this option to access the update module that manages updates to the virus signature database.

Setup – Select this option to adjust your computer's security level. If the Advanced mode is activated, the submenus Antivirus and antispyware protection, Personal firewall, and Antispam module will appear.

Tools – This option is available only in Advanced mode. Provides access to Log files, Quarantine and the Scheduler.

Help and support – Select this option to access help files, the ESET Knowledgebase, ESET's web site and access a Customer Care support request.

The ESET Smart Security user interface allows users to toggle Standard and Advanced modes. To toggle between modes, see the **Display** link located in the bottom left corner of the main ESET Smart Security window. Click this button to select the desired display mode.



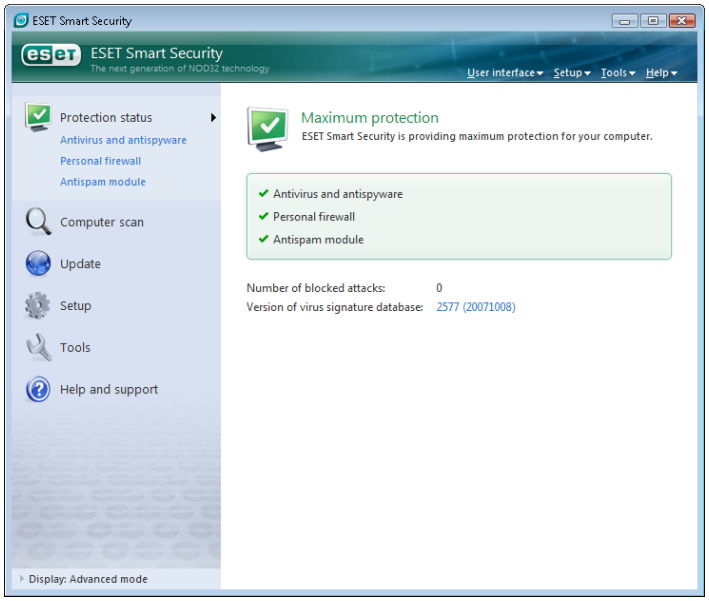
The Standard mode provides access to features required for common operations. It does not display any advanced options.

Toggling to Advanced mode adds the **Tools** option to the main menu. The Tools option allows the user to access Scheduler, Quarantine, or view ESET Smart Security Log files.

NOTE: All remaining instructions in this guide will take place in Advanced mode.

3.1.1 Checking operation of the system

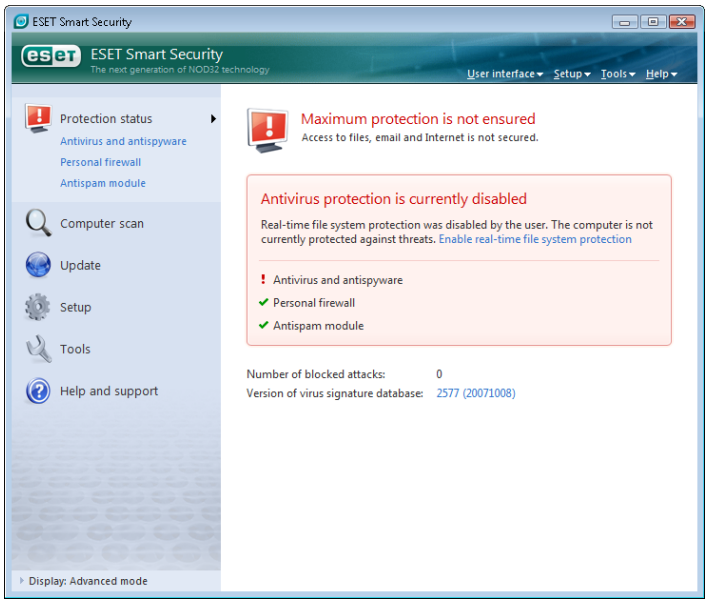
To view the **Protection status**, click this option at the top of the main menu. A status summary about the operation of ESET Smart Security will be displayed on the right side of the window, and a submenu with three items appears: **Antivirus and antispyware**, **Personal firewall**, and **Antispam module**. Select any of these to view more detailed information about a given protection module.



If the modules enabled are working properly, they are assigned a green check. If not, a red exclamation point or orange notification icon is displayed, and additional information about the module is shown in the upper part of the window. A suggested solution for fixing the module is also displayed. To change the status of individual modules, click **Setup** in the main menu and click on the desired module.

3.1.2 What to do if the program doesn't work properly

If ESET Smart Security detects a problem in any of its protection modules, it is reported in the **Protection status** window. A potential solution to the problem is also offered here.

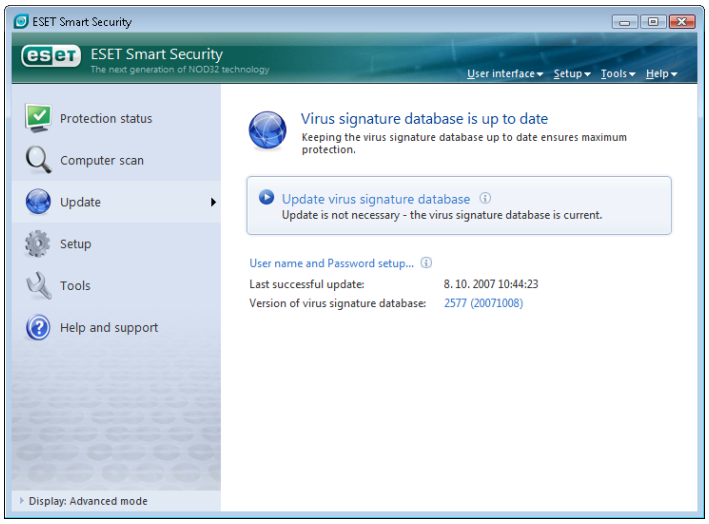


If it is not possible to solve a problem using the displayed list of known problems and solutions, click **Help and support** to access the help files or search the Knowledgebase. If a solution still cannot be found, you can submit a support request to ESET Customer Care. Based on this feedback, our specialists can quickly respond to your questions and effectively advise you on the problem.

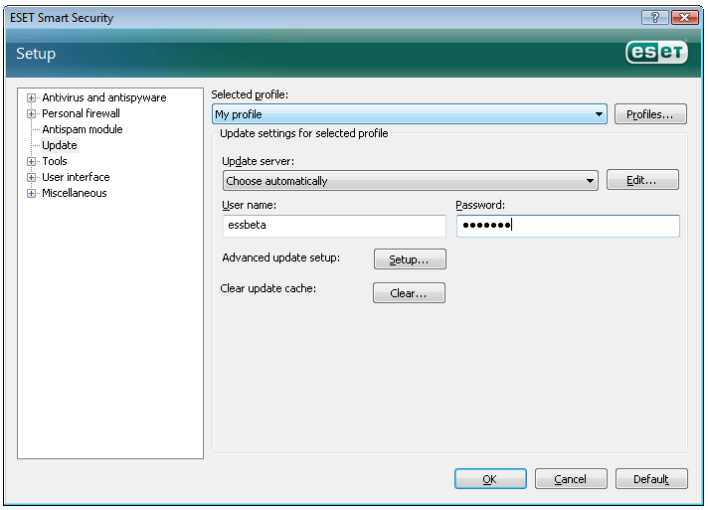
3.2 Update setup

Updating the virus signature database and updating program components are an important part of providing complete protection against malicious code. Please pay special attention to their configuration and operation. From the main menu, select **Update** and then click **Update virus signature database** in the main program window to instantly check for availability of a newer database update. **User name and Password setup...** displays a dialog box where the User name and Password received at the time of purchase should be entered.

If the User name and Password were entered during the installation of ESET Smart Security you will not be prompted for them at this point.

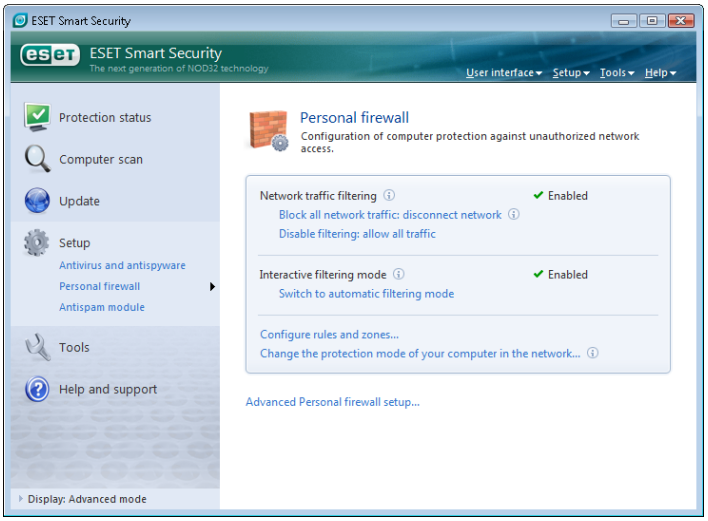


The **Advanced Setup** window (to access, press F5) contains other detailed update options. The **Update server:** drop-down menu should be set to **Choose automatically**. To configure advanced update options such as the update mode, proxy server access, accessing updates on a local server and creating virus signature copies (ESET Smart Security Business Edition), click the **Setup...** button.

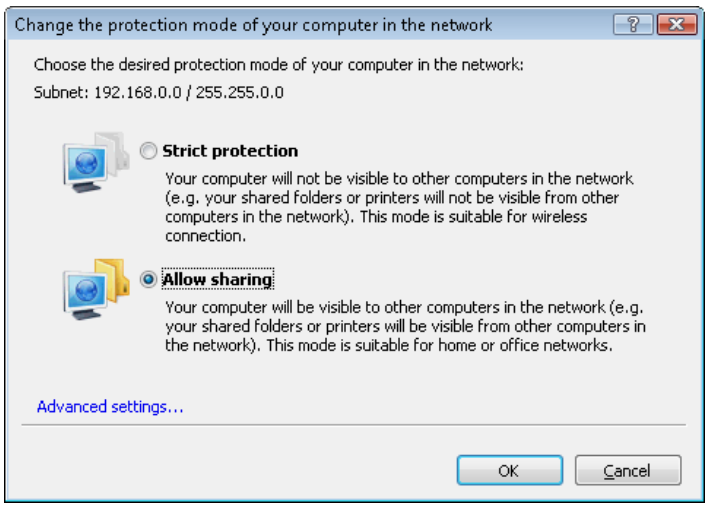


3.3 Trusted zone setup

Configuration of a Trusted zone is an important step in protecting your computer in a network environment. You can allow other users to access your computer by configuring the Trusted zone to allow sharing. Click **Setup > Personal firewall > Change the protection mode of your computer in the network...** A window will be displayed, allowing you to configure the settings of your computer protection mode in the actual network/zone.



Trusted Zone detection is performed after installation of ESET Smart Security and whenever the computer is connected to a new network. Therefore, there is no need to define the Trusted zone in most cases. By default, there is a dialog window displayed upon detection of a new zone which allows you to set the protection level for that zone.

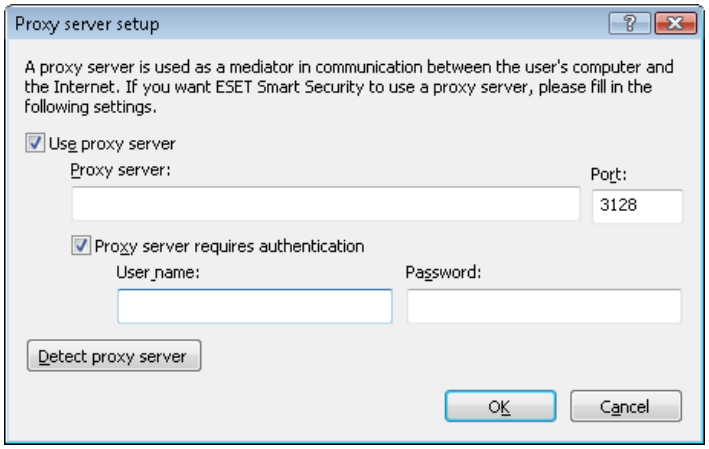

Change the protection mode of your computer in the network
Choose the desired protection mode of your computer in the network:
Subnet: 192.168.0.0 / 255.255.0.0
Strict protection
Your computer will not be visible to other computers in the network (e.g. your shared folders or printers will not be visible from other computers in the network). This mode is suitable for wireless connection.
Allow sharing
Your computer will be visible to other computers in the network (e.g. your shared folders or printers will be visible from other computers in the network). This mode is suitable for home or office networks.
Advanced settings...
OK
Cancel

Warning! An incorrect trusted zone configuration may pose a security risk to your computer.

NOTE: By default, workstations from a Trusted zone are granted access to shared files and printers, incoming RPC communication is enabled, and remote desktop sharing is also available.

3.4 Proxy server setup

If you use a proxy server to mediate connection to the Internet on a system using ESET Smart Security, it must be specified in Advanced Setup (F5). To access the **Proxy server** configuration window, click **Miscellaneous > Proxy server** from the Advanced Setup tree. Select the **Use proxy server** check box, and enter the IP address and port of the proxy server, along with its authentication data.


Proxy server setup
A proxy server is used as a mediator in communication between the user's computer and the Internet. If you want ESET Smart Security to use a proxy server, please fill in the following settings.
Use proxy server
Proxy server:
Port:
3128
Proxy server requires authentication
User name:
Password:
Detect proxy server
OK
Cancel

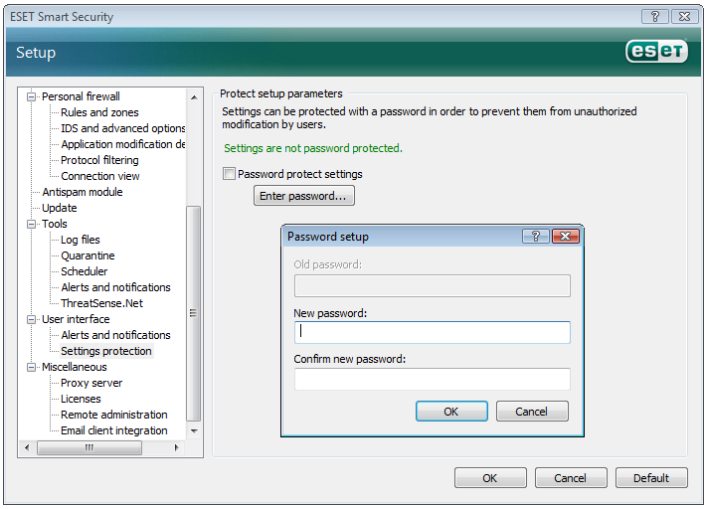
If this information is not available, you can attempt to automatically detect proxy server settings for ESET Smart Security by clicking the **Detect proxy server** button.

NOTE: Proxy server options for various update profiles may differ. If this is the case, configure the proxy server in the advanced update setup.

3.5 Settings protection

ESET Smart Security Settings can be very important from the perspective of your organization's security policy. Unauthorized modifications can potentially endanger the stability and protection of your system. To password protect the setup parameters, start from the main menu and click **Setup > Enter entire advanced setup tree... > User interface > Settings protection** and click the **Enter password...** button.

Enter a password, confirm it by typing it again, and click **OK**. This password will be required for any future modifications to ESET Smart Security settings.



4. Work with ESET Smart Security

4.1 Antivirus and antispyware protection

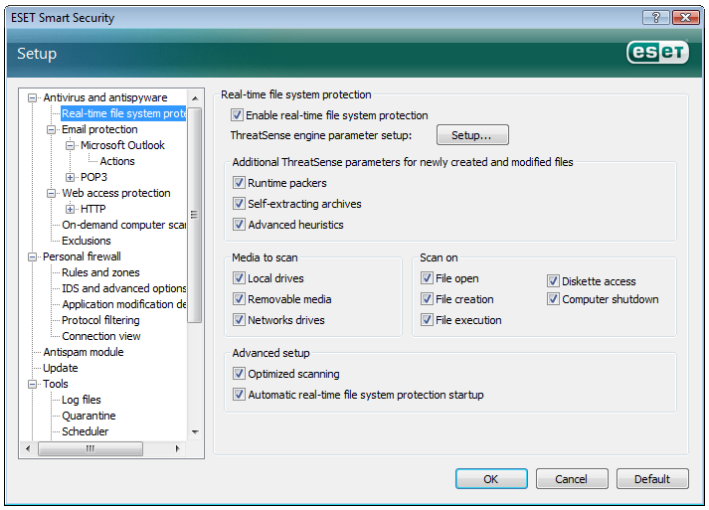
Antivirus protection guards against malicious system attacks by controlling file, email and Internet communication. If a threat with malicious code is detected, the Antivirus module can eliminate it by first blocking it, and then cleaning, deleting or moving it to quarantine.

4.1.1 Real-time file system protection

Real-time file system protection controls all antivirus-related events in the system. All files are scanned for malicious code at the moment they are opened, created or run on the computer. Real-time file system protection is launched at system startup.

4.1.1.1 Control setup

The real-time file system protection checks all types of media, and control is triggered by various events. Control utilizes the ThreatSense technology detection methods (as described in ThreatSense engine parameter setup). The control behavior may vary for newly created files and existing files. For newly created files, it is possible to apply a deeper level of control.



4.1.1.1.1 Media to scan

By default, all types of media are scanned for potential threats.

Local drives – Controls all system hard drives
Removable media – Diskettes, USB storage devices, etc.
Network drives – Scans all mapped drives

We recommend that you keep the default settings and only modify them in specific cases, such as when scanning certain media significantly slows data transfers.

4.1.1.1.2 Scan on (Event-triggered scanning)

By default, all files are scanned upon opening, execution or creation. We recommend that you keep the default settings, as these provide the maximum level of real-time protection for your computer.

The **Diskette access** option provides control of the diskette boot sector when this drive is accessed. The **Computer shutdown** option provides control of the hard disk boot sectors during computer shutdown. Although boot viruses are rare today, we recommend that you leave these options enabled, as there is still the possibility of infection by a boot virus from alternate sources.

4.1.1.1.3 Additional ThreatSense parameters for newly created files

The probability of infection in newly-created files is comparatively higher than in existing files. This is why the program checks these files with additional scanning parameters. Along with common signature-based scanning methods, advanced heuristics are used, which greatly improves detection rates. In addition to newly-created files, scanning is also performed on self-extracting files (SFX) and runtime packers (internally compressed executable files).

4.1.1.1.4 Advanced setup

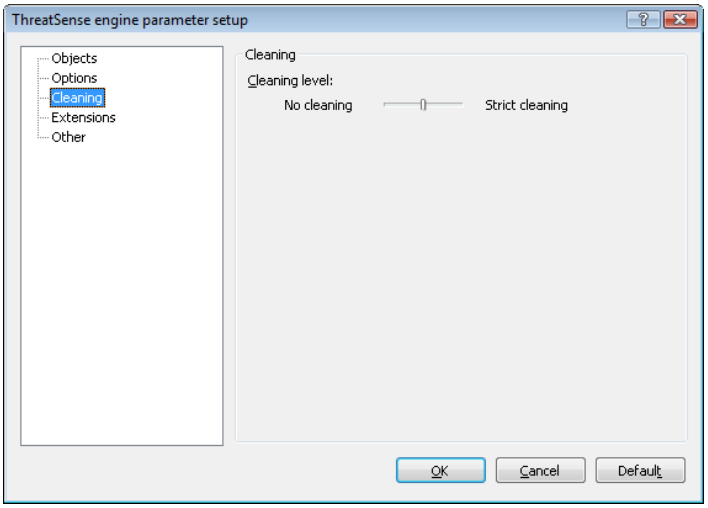
To provide the minimum system footprint when using real-time protection, files which have already been scanned are not scanned repeatedly (unless they have been modified). Files are scanned again immediately after each virus signature database update. This behavior is configured using the **Optimized scanning** option. If this is disabled, all files are scanned each time they are accessed.

By default, Real-time protection is launched at operating system startup time and provides uninterrupted scanning. In special cases (e.g., if there is a conflict with another real-time scanner), the real-time protection can be terminated by disabling the **Automatic real-time file system protection startup** option.

4.1.1.2 Cleaning levels

The real-time protection has three cleaning levels (to access, click the **Setup...** button in the **Real-time file system protection** section and then click the **Cleaning** branch).

- The first level displays an alert window with available options for each infiltration found. The user must choose an action for each infiltration individually. This level is designed for more advanced users who know which steps to take in the event of an infiltration.
- The default level automatically chooses and performs a predefined action (depending on the type of infiltration). Detection and deletion of an infected file is signaled by an information message located in the bottom right corner of the screen. However, an automatic action is not performed if the infiltration is located within an archive which also contains clean files, and it is not performed on objects for which there is no predefined action.
- The third level is the most "aggressive" – all infected objects are cleaned. As this level could potentially result in the loss of valid files, we recommend that it be used only in specific situations.



4.1.1.3 When to modify the real-time protection configuration

Real-time protection is the most essential component of maintaining a secure system. Therefore, please be careful when modifying its parameters. We recommend that you only modify its parameters in specific cases. For example, if there is a conflict with a certain application or real-time scanner of another antivirus program.

After installation of ESET Smart Security, all settings are optimized to provide the maximum level of system security for users. To restore the default settings, click the **Default** button located at the bottom-right of the **Real-time file system protection** window (**Advanced Setup > Antivirus and antispyware > Real-time file system protection**).

4.1.1.4 Checking real-time protection

To verify that real-time protection is working and detecting viruses, use a test file from eicar.com. This test file is a special harmless file detectable by all antivirus programs. The file was created by the EICAR company (European Institute for Computer Antivirus Research) to test the functionality of antivirus programs. The file eicar.com is available for download at http://www.eicar.org/download/eicar.com

NOTE: Before performing a real-time protection check, it is necessary to disable the firewall. If the firewall is enabled, it will detect the file and prevent test files from downloading.

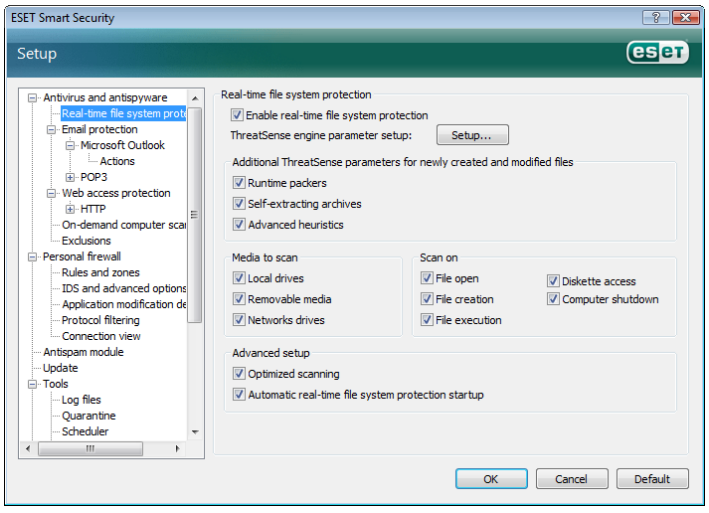
4.1.1.5 What to do if the real-time protection does not work

In the next chapter, we describe problem situations that may arise when using real-time protection, and how to troubleshoot them.

Real-time protection is disabled

If real-time protection was inadvertently disabled by a user, it needs to be reactivated. To reactivate real-time protection, navigate to **Setup > Antivirus and antispyware** and click **Enable** in the **Real-time file system protection** section of the main program window.

If real-time protection is not initiated at system startup, it is probably due to the disabled option **Automatic real-time file system protection startup**. To enable this option, navigate to **Advanced Setup** (F5) and click **Real-time file system protection** in the Advanced Setup tree. In the **Advanced setup** section at the bottom of the window, make sure that the **Automatic real-time file system protection startup** check box is selected.



If Real-time protection does not detect and clean infiltrations

Make sure that no other antivirus programs are installed on your computer. If two real-time protection shields are enabled at the same time, they may conflict with each other. We recommend that you uninstall any other antivirus programs on your system.

Real-time protection does not start

If real-time protection is not initiated at system startup (and the **Automatic real-time file system protection startup** option is enabled), it may be due to conflicts with other programs. If this is the case, please consult ESET's Customer Care specialists.

4.1.2 Email protection

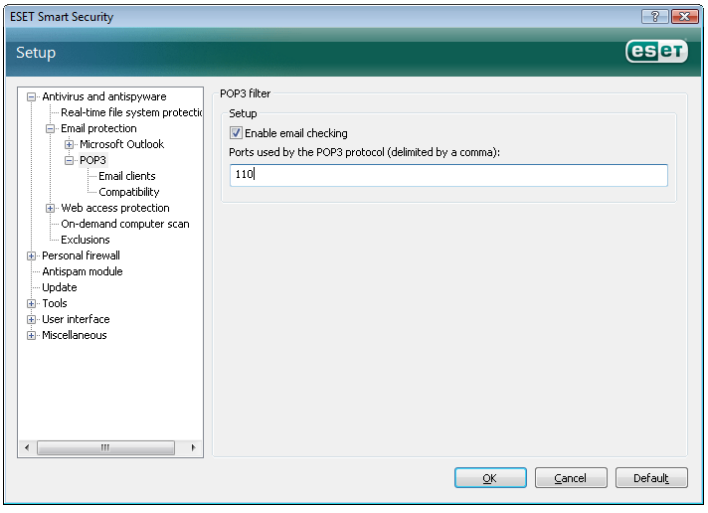
Email protection provides control of email communication received through the POP3 protocol. Using the plug-in program for Microsoft Outlook, ESET Smart Security provides control of all communications from the email client (POP3, MAPI, IMAP, HTTP). When examining incoming messages, the program uses all advanced scanning methods provided by the ThreatSense scanning engine. This means that detection of malicious programs takes place even before being matched against the virus signature database. Scanning of POP3 protocol communications is independent of the email client used.

4.1.2.1 POP3 checking

The POP3 protocol is the most widespread protocol used to receive email communication in an email client application. ESET Smart Security provides protection of this protocol regardless of the email client used.

The module providing this control is automatically initiated at operating system startup time and is then active in memory. For the module to work correctly, please make sure it is enabled – POP3 checking is performed automatically with no need for reconfiguration of the email client. By default, all communication on port 110 is scanned, but other communication ports can be added if necessary. Port numbers must be delimited by a comma.

Encrypted communication is not controlled.



4.1.2.1.1 Compatibility

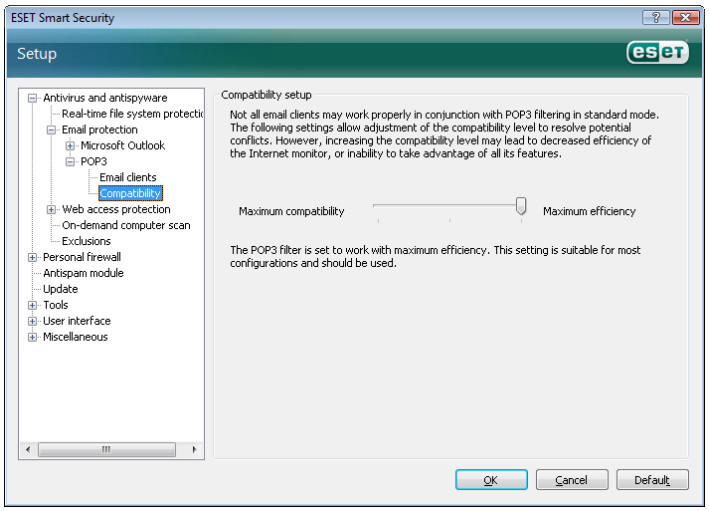
Certain email programs may experience problems with POP3 filtering (e.g. if receiving messages with a slow Internet connection, timeouts may occur due to checking). If this is the case, try modifying the way control is performed. Decreasing the control level may improve the speed of the cleaning process. To adjust the control level of POP3 filtering, navigate to **Antivirus and antispyware > Email protection > POP3 > Compatibility**.

If **Maximum efficiency** is enabled, infiltrations are removed from infected messages and information about the infiltration is inserted before the original email subject (the options **Delete** or **Clean** must be activated, or **Strict** or **Default** cleaning level must be enabled)

Medium compatibility modifies the way messages are received. Messages are gradually sent to the email client – after the last part of the message is transferred, it will be scanned for infiltrations.

However, the risk of infection increases with this level of control. The level of cleaning and the handling of tag messages (notification alerts which are appended to the subject line and body of emails) is identical to the maximum efficiency setting.

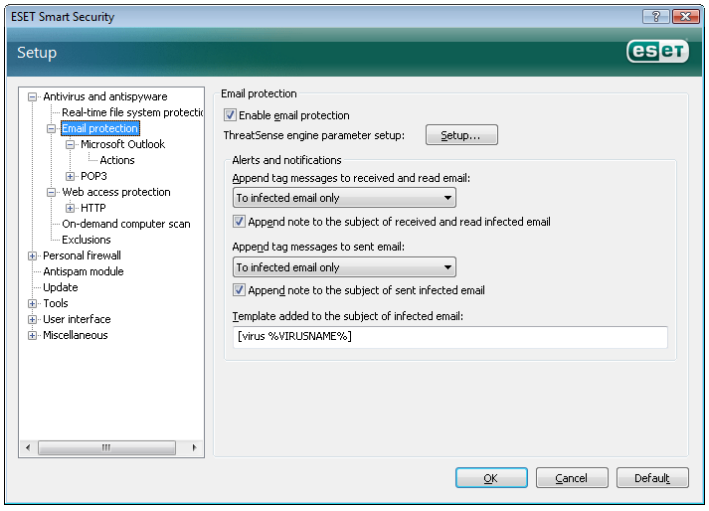
With the **Maximum compatibility** level, the user is warned by an alert window which reports the receipt of an infected message. No information about infected files is added to the subject line or to the email body of delivered messages and infiltrations are not automatically removed. Deleting infiltrations must be performed by the user from the email client.


ESET Smart Security
Setup
eset
Antivirus and antispyware
Real-time file system protectic
Email protection
Microsoft Outlook
POP3
Email clients
Compatibility
Web access protection
On-demand computer scan
Exclusions
Personal firewall
Antispam module
Update
Tools
User interface
Miscellaneous
Compatibility setup
Not all email clients may work properly in conjunction with POP3 filtering in standard mode. The following settings allow adjustment of the compatibility level to resolve potential conflicts. However, increasing the compatibility level may lead to decreased efficiency of the Internet monitor, or inability to take advantage of all its features.
Maximum compatibility
Maximum efficiency
The POP3 filter is set to work with maximum efficiency. This setting is suitable for most configurations and should be used.
OK
Cancel
Default

4.1.2.2 Integration with Microsoft Outlook, Outlook Express, and Windows Mail

Integration of ESET Smart Security with email clients increases the level of active protection against malicious code in email messages. If your email client is supported, this integration can be enabled in ESET Smart Security. If integration is activated, the ESET Smart Security Antispam toolbar is inserted directly into the email client, allowing for more efficient email protection. The integration settings are available through **Setup > Enter entire advanced setup tree... > Miscellaneous >Email client integration**. This dialog window allows you to activate integration with the supported email clients. Email clients which are currently supported include Microsoft Outlook, Outlook Express and Windows Mail.

Email protection is started by the activation of the **Enable email protection** check box in **Advanced Setup (F5)** > **Antivirus and antispyware** > **Email protection**.



4.1.2.2.1 Appending tag messages to email body

Each email controlled by ESET Smart Security can be marked by appending a tag message to the subject or email body. This feature increases the level of credibility for the addressee and if an infiltration is detected, it provides valuable information about the threat level of a given email/sender.

The options for this functionality are available through **Advanced setup > Antivirus and antispyware protection > Email protection**. The program can **Append tag messages to received and read mail**, as well as **Append tag messages to sent mail**. Users also have the ability to decide whether tag messages should be appended to all email, to infected email only, or not at all. ESET Smart Security also allows the user to append messages to the original subject of infected messages. To enable appending to the subject, select the options **Append note to the subject of received and read infected email** and **Append note to the subject of sent infected email**.

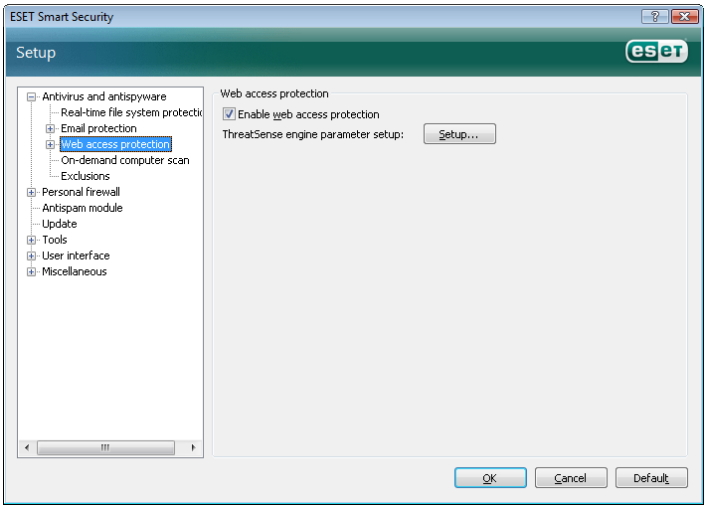
The content of the notifications can be modified in the Template field added to the subject of infected email. The above-mentioned modifications can help to automate the process of filtering infected email, as it allows you to filter email with a specific subject (if supported in your email client) to a separate folder.

4.1.2.3 Removing infiltrations

If an infected email message is received, an alert window is displayed. The alert window shows the sender name, the email, and name of the infiltration. In the lower part of the window, the options **Clean**, **Delete** or **Leave** are available for the detected object. In almost all cases, we recommend that you select either **Clean** or **Delete**. In special situations, when you wish to receive the infected file, select **Leave**. If **Strict cleaning** is enabled, an information window with no options available for infected objects is displayed.

4.1.3 Web access protection

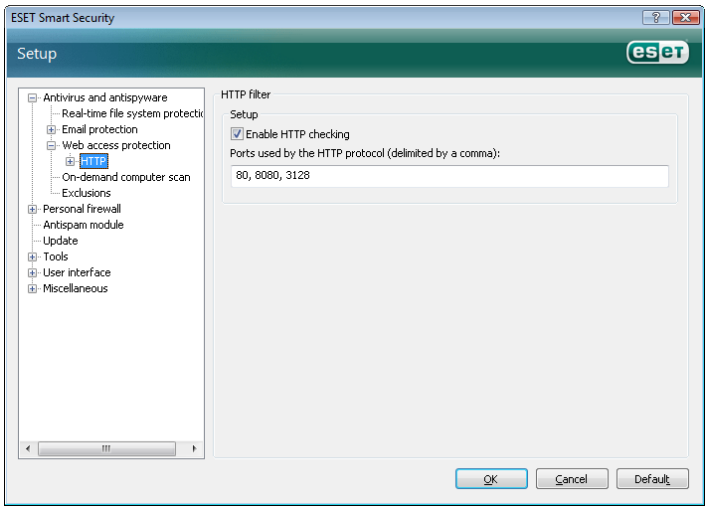
Internet connectivity is a standard feature in a personal computer. Unfortunately, it has also become the main medium for transferring malicious code. Because of this, it is essential that you carefully consider your Web access protection. We strong recommend that the **Enable web access protection** option is activated. This option is located in **Advanced Setup (F5) > Antivirus and antispyware protection > Web access protection**.



4.1.3.1 HTTP

Web access protection's primary function is to monitor the communication between Internet browsers and remote servers, according to the rules of the HTTP (Hypertext Transfer Protocol) protocol. ESET Smart Security is by default configured to use the HTTP standards of most Internet browsers. However, the HTTP checking

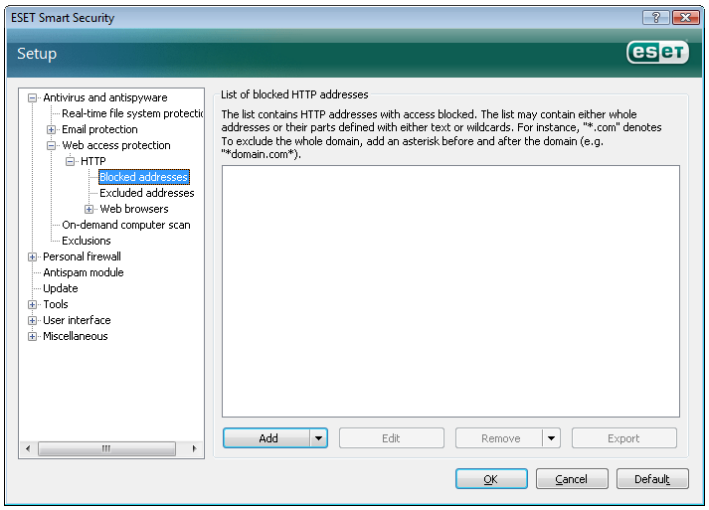
setup options can be partially modified in the section **Web access protection > HTTP**. In the **HTTP filter Setup** window, you can enable or disable HTTP checking with the option **Enable HTTP checking**. You can also define the port numbers which are used by the system for the HTTP communication. By default, the port numbers 80, 8080 and 3128 are used. HTTP traffic on any port can be automatically detected and scanned, by adding additional port numbers, separated by a comma.



4.1.3.1.1 Blocked / excluded addresses

The HTTP checking setup allows you to create user-defined lists of **Blocked** and **Excluded** URL (Uniform Resource Locator) **addresses**.

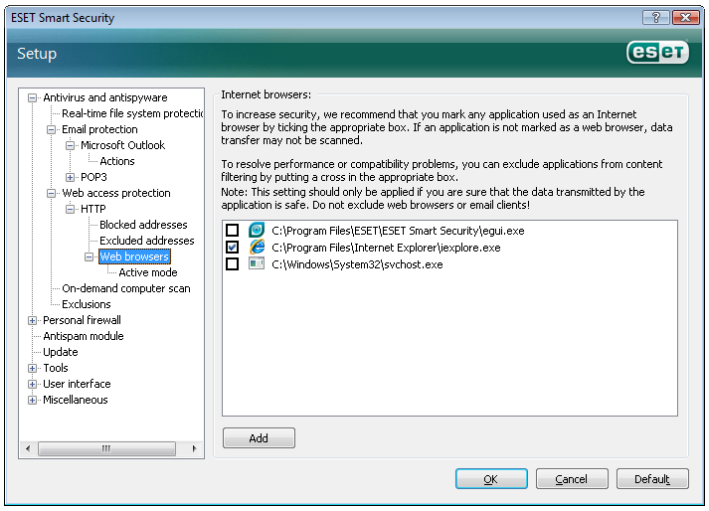
Both dialog windows contain the buttons **Add**, **Edit**, **Remove** and **Export**, allowing you to easily manage and maintain the lists of specified addresses. If an address requested by the user is in the list of blocked addresses, it will not be possible to access the address. On the other hand, addresses in the list of excluded addresses are accessed with no checking for malicious code. In both lists, the special symbols * (asterisk) and **?** (question mark) can be used. The asterisk substitutes any character string, and the question mark any symbol. Particular care should be taken when specifying excluded addresses, because the list should only contain trusted and safe addresses. Similarly, it is necessary to make sure that the symbols * and **?** are used correctly in this list.



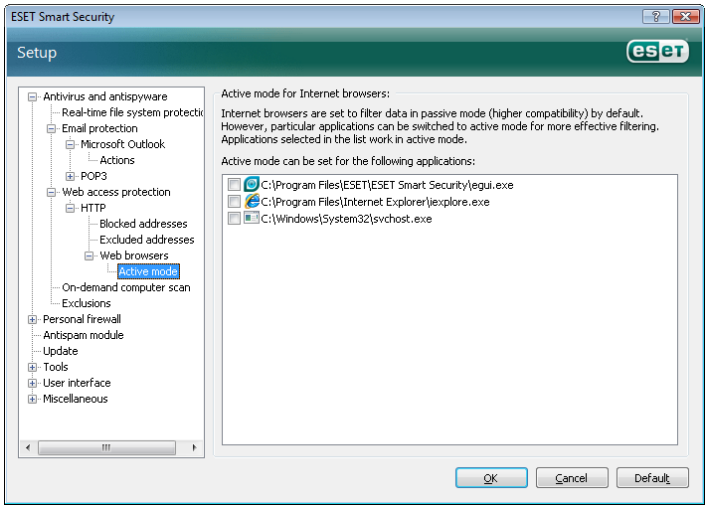
4.1.3.1.2 Web browsers

ESET Smart Security also contains the **Web browsers** feature, which allows the user to define whether the given application is a browser or not. If an application is marked as a browser by the user, all communication from this application is monitored regardless of the port numbers involved in the communication.

The Web browsers feature complements the HTTP checking feature, as HTTP checking only takes place on predefined ports. However, many Internet services utilize dynamically changing or unknown port numbers. To account for this, the Web browser feature can establish control of port communications regardless of the connection parameters.


ESET Smart Security
Setup
Antivirus and antispyware
Real-time file system protecti
Email protection
Microsoft Outlook
Actions
POP3
Web access protection
HTTP
Blocked addresses
Excluded addresses
Web browsers
Active mode
On-demand computer scan
Exclusions
Personal firewall
Antispam module
Update
Tools
User interface
Miscellaneous
Internet browsers:
To increase security, we recommend that you mark any application used as an Internet browser by ticking the appropriate box. If an application is not marked as a web browser, data transfer may not be scanned.
To resolve performance or compatibility problems, you can exclude applications from content filtering by putting a cross in the appropriate box.
Note: This setting should only be applied if you are sure that the data transmitted by the application is safe. Do not exclude web browsers or email clients!
C:\Program Files\ESET\ESET Smart Security\egui.exe
C:\Program Files\Internet Explorer\iexplore.exe
C:\Windows\System32\svchost.exe
Add
OK
Cancel
Default

The list of applications marked as browsers is accessible directly from the **Web browsers** submenu of the **HTTP** branch. This section also contains the submenu **Active mode**, which defines the checking mode for Internet browsers. The **Active mode** is useful because it examines transferred data as a whole. If it is not enabled, communication of applications is monitored gradually in batches. This decreases the effectiveness of the data verification process, but it also provides higher compatibility for the listed applications. If no problems occur while using it, we recommend that you enable the active checking mode by selecting the check box next to the desired application.



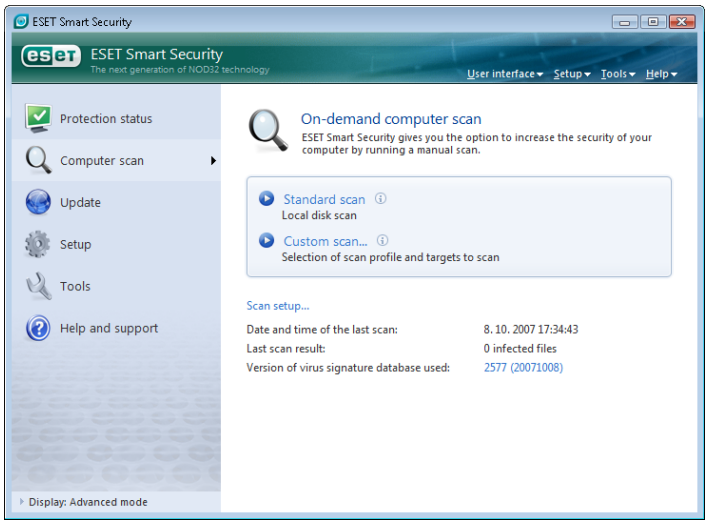
4.1.4 Computer scan

If you suspect that your computer is infected (it behaves abnormally), run an On-demand computer scan to examine your computer for infiltrations. From a security point of view, it is essential that computer scans are not just run when an infection is suspected, but regularly as part of routine security measures. Regular scanning provides detection of infiltrations which were not detected by the real-time scanner at the time they were saved to the disk. This can happen if the real-time scanner was disabled at the time of infection, or if the virus signature database is obsolete.

We recommend that you run an On-demand scan at least once or twice a month. Scanning can be configured as a scheduled task through **Tools > Scheduler**.

4.1.4.1 Type of scan

Two types are available. The **Standard scan** quickly scans the system with no need for further configuration of the scan parameters. The **Custom scan**... allows the user to select any of the predefined scan profiles, as well as choose scan objects from the tree structure.



4.1.4.1.1 Standard scan

Standard scan is a user-friendly method which allows the user to quickly launch a computer scan and clean infected files with no need for user intervention. Its main advantages are easy operation with no detailed scanning configuration. Standard scan checks all files on local drives (excluding email and archive files) and automatically cleans or deletes detected infiltrations. The cleaning level is automatically set to the default value. For more detailed information on types of cleaning, see Cleaning (see page 18).

The standard scanning profile is designed for users who wish to quickly and easily scan their computers. It offers an effective scanning and cleaning solution without requiring an extensive configuration process.

4.1.4.1.2 Custom scan

Custom scan is an optimal solution if you wish to specify scanning parameters such as scan targets and scanning methods. The advantage of Custom scan is the ability to configure the parameters in detail. The configurations can be saved to user-defined scan profiles, which can be useful if scanning is repeatedly performed with the same parameters.

To select scan targets, use the drop-down menu of the quick target selection feature or select targets from the tree structure listing all devices available on the computer. Furthermore, you can choose from three cleaning levels by clicking **Setup... > Cleaning**. If you are only interested in scanning the system with no additional actions performed, select the **Scan without cleaning** check box.

Performing computer scans using the Custom scan mode is suitable for advanced users with previous experience using antivirus programs.

4.1.4.2 Scan targets

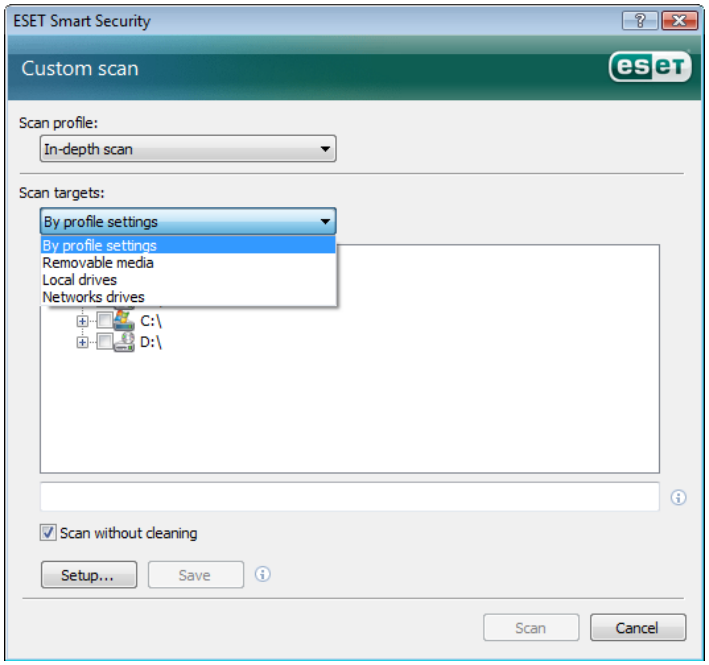
The Scan targets drop-down menu allows you to select files, folders and devices (disks) to be scanned for viruses.

Using the quick scan targets menu option, you can select the following targets:

Local drives – controls all system hard drives

Removable media – diskettes, USB storage devices, CD/DVD

Network drives – all mapped drives



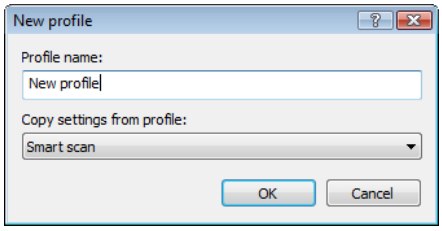
A scan target can also be more precisely specified by entering the path to the folder or file(s) you wish to include in scanning. Select targets from the tree structure listing all devices available on the computer.

4.1.4.3 Scan profiles

The preferred computer scan parameters can be saved to profiles. The advantage of creating scan profiles is that they can be used regularly for scanning in the future. We recommend that you create as many profiles (with various scan targets, scan methods and other parameters) as the user regularly uses.

To create a new profile that can be used repeatedly for future scans, navigate to **Advanced setup** (F5) **> On-demand computer scan**. Click the **Profiles...** button on the right to display the list of existing scan profiles and the option to create a new one. The following **ThreatSense engine parameters setup** describe each parameter of the scan setup. This will help you create a scan profile to fit your needs.

Example:
Suppose that you want to create your own scan profile and the configuration assigned to the profile **Smart scan** is partially suitable. But you don't want to scan runtime packers or potentially unsafe applications and you also want to apply **Strict cleaning**. From the **Configuration profiles** window, click the **Add...** button. Enter the name of your new profile in the **Profile name** field, and select **Smart scan** from the **Copy settings from profile:** drop-down menu. Then adjust the remaining parameters to meet your requirements.



4.1.5 ThreatSense engine parameters setup

ThreatSense is the name of the technology consisting of complex threat detection methods. This technology is proactive, which means it also provides protection during the early hours of the spread of a new threat. It uses a combination of several methods (code analysis, code emulation, generic signatures, virus signatures) which work

in concert to significantly enhance system security. The scanning engine is capable of controlling several data streams simultaneously, maximizing the efficiency and detection rate. ThreatSense technology also successfully eliminates rootkits.

The ThreatSense technology setup options allow the user to specify several scan parameters:

- File types and extensions that are to be scanned
- The combination of various detection methods
- Levels of cleaning, etc.

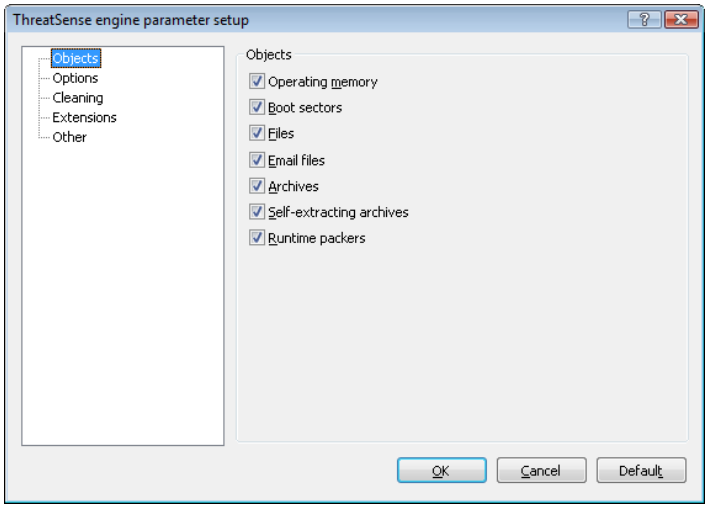
To enter the setup window, click the **Setup...** button located in any module's setup window which uses ThreatSense technology (see below). Different security scenarios could require different configurations. With this in mind, ThreatSense is individually configurable for the following protection modules:

- Real-time file system protection
- System startup file check
- Email protection
- Web access protection
- On-demand computer scan

The ThreatSense parameters are highly optimized for each module, and their modification can significantly influence system operation. For example, changing parameters to always scan runtime packers, or enabling advanced heuristics in the real-time file system protection module could result in a system slow-down (normally, only newly-created files are scanned using these methods). Therefore, we recommend that you leave the default ThreatSense parameters unchanged for all modules except Computer scan.

4.1.5.1 Objects setup

The **Objects** section allows you to define which computer components and files will be scanned for infiltrations.



Operating memory – Scans for threats that attack the operating memory of the system.

Boot sectors – Scans boot sectors for the presence of viruses in the master boot record

Files – Provides scanning of all common file types (programs, pictures, audio, video files, database files, etc.)

Email files – Scans special files where email messages are contained

Archives – Provides scanning of files compressed in archives (.rar, .zip, .arj, .tar, etc.)

Self-extracting archives – Scans files which are contained in self-extracting archive files, but typically presented with a .exe extension

Runtime packers – runtime packers (unlike standard archive types) decompress in memory, in addition to standard static packers (UPX, yoda, ASPack, FGS, etc.).

4.1.5.2 Options

In the **Options** section, the user can select the methods to be used when scanning the system for infiltrations. The following options are available:

Signatures – Signatures can exactly and reliably detect and identify infiltrations by their name using virus signatures.

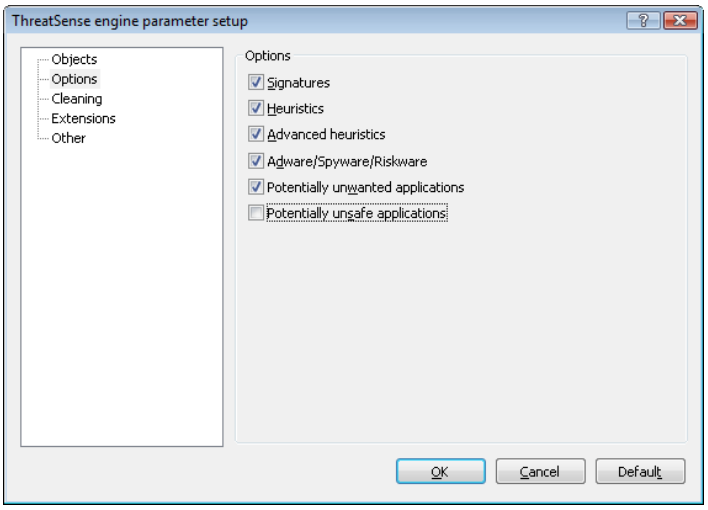
Heuristics – Heuristics is an algorithm that analyzes the (malicious) activity of programs. The main advantage of heuristic detection is the ability to detect new malicious software which did not previously exist, or was not included in the list of known viruses (virus signatures database).

Advanced heuristics – Advanced heuristics comprise a unique heuristic algorithm developed by ESET optimized for detecting computer worms and trojan horses written in high level programming languages. Due to advanced heuristics, the detection intelligence of the program is significantly higher.

Adware/Spyware/Riskware – This category includes software which collects various sensitive information about users without their informed consent. This category also includes software which displays advertising material.

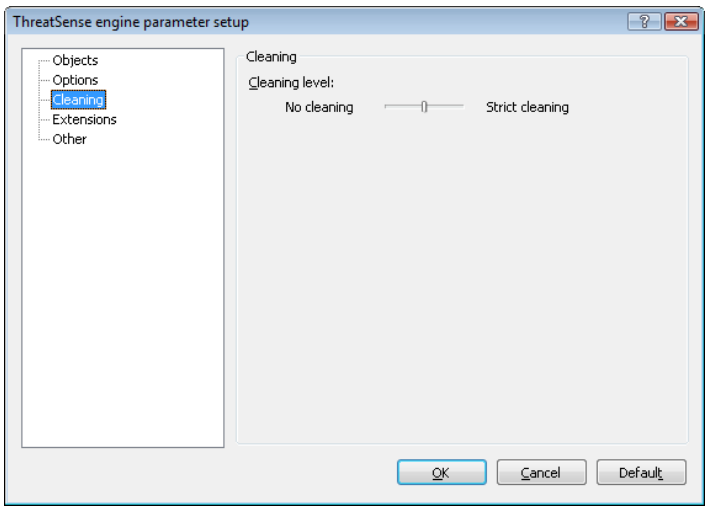
Potentially unsafe applications – Potentially unsafe applications is the classification used for commercial, legitimate software. It includes programs such as remote access tools, which is why this option is disabled by default.

Potentially unwanted applications – Potentially unwanted applications are not necessarily intended to be malicious, but they may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes include unwanted pop-up windows, activation and running of hidden processes, increased usage of system resources, changes in search results, and applications communicating with remote servers.



4.1.5.3 Cleaning

The cleaning settings determine the behavior of the scanner during the cleaning of infected files. There are 3 levels of cleaning:



No cleaning
Infected files are not cleaned automatically. The program will display a warning window and allow the user to choose an action.

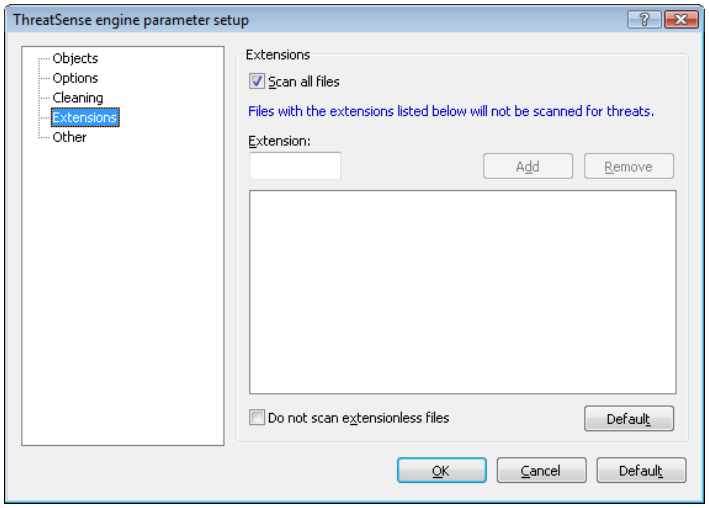
Default level
The program will attempt to automatically clean or delete an infected file. If it is not possible to select the correct action automatically, the program will offer a choice of follow-up actions. The choice of follow-up actions will also be displayed if a predefined action could not be completed.

Strict cleaning
The program will clean or delete all infected files (including archives). The only exceptions are system files. If it is not possible to clean them, the user is offered an action to take in a warning window.

Warning:
In the Default mode, the entire archive file is deleted only if all files in the archive are infected. If the archive also contains legitimate files, it will not be deleted.If an infected archive file is detected in the Strict cleaning mode, the entire archive will be deleted, even if clean files are present.

4.1.5.4 Extensions

An extension is part of the file name delimited by a period. The extension defines the type and content of the file. This section of the ThreatSense parameter setup lets you define the types of files to scan.



By default, all files are scanned regardless of their extension. Any extension can be added to the list of files excluded from scanning. If the **Scan all files** option is unchecked, the list changes to show all currently scanned file extensions. Using the **Add** and **Remove** buttons, you can enable or prohibit scanning of desired extensions.

To enable scanning of files with no extension, select the **Scan extensionless files** option.

Excluding files from scanning has its purpose if the scanning of certain file types prevents the program using the extensions to run properly. For example, it may be advisable to exclude the .edb, .eml and .tmp extensions when using the MS Exchange server.

4.1.6 An infiltration is detected

Infiltrations can reach the system from various entry points; web pages, shared folders, via email, or from removable computer devices (USB, external disks, CDs, DVDs, diskettes, etc.).

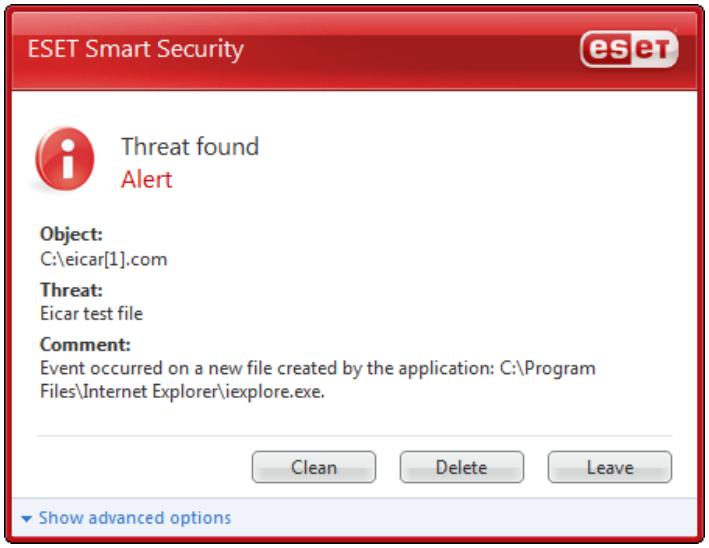
If your computer is showing signs of malware infection, e.g. it is slower, often freezes, etc., we recommend that you do the following:

- Open ESET Smart Security and click **Computer scan**
- Click **Standard scan** (for more information, see Standard scan).
- After the scan has finished, review the log for the number of scanned, infected and cleaned files.

If you only wish to scan a certain part of your disk, click **Custom scan** and select targets to be scanned for viruses.

As a general example of how infiltrations are handled in ESET Smart Security, suppose that an infiltration is detected by the real-time file system monitor, which uses the Default cleaning level. It will attempt to clean or delete the file. If there is no pre-defined action to take for the real-time protection module, you will be asked to select an option in an alert window. Usually, the options **Clean**, **Delete** and **Leave** are available. Selecting **Leave** is not recommended, since the infected file(s) would be left untouched. The exception to this is when you are sure that the file is harmless and has been detected by mistake.

Cleaning and deleting
Apply cleaning if a clean file has been attacked by a virus which has attached malicious code to the cleaned file. If this is the case, first attempt to clean the infected file in order to restore it to its original state. If the file consists exclusively of malicious code, it will be deleted.



If an infected file is "locked" or in use by a system process, it will usually only be deleted after it is released (normally after a system restart).

Deleting files in archives
In the Default cleaning mode, the entire archive will be deleted only if it contains infected files and no clean files. In other words, archives are not deleted if they also contain harmless clean files. However, use caution when performing a Strict cleaning scan – with Strict cleaning the archive will be deleted if it contains at least one infected file, regardless of the status of other files in the archive.

4.2 Personal firewall

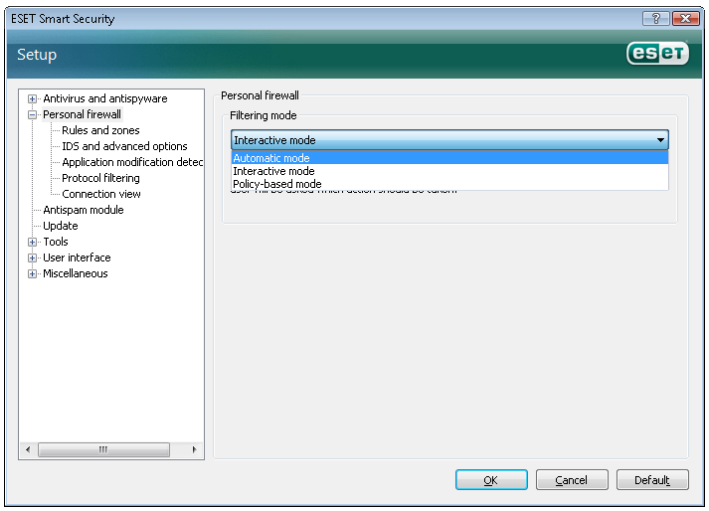
The Personal firewall controls all network traffic to and from the system. This is accomplished by allowing or denying individual network connections based on specified filtering rules. It provides protection against attacks from remote computers and enables blocking of some services. It also provides antivirus protection for HTTP and POP3 protocols. This functionality represents a very important element of computer security.

4.2.1 Filtering modes

Three filtering modes are available for the ESET Smart Security Personal firewall. The behavior of the firewall changes based on the selected mode. Filtering modes also influence the level of user interaction required.

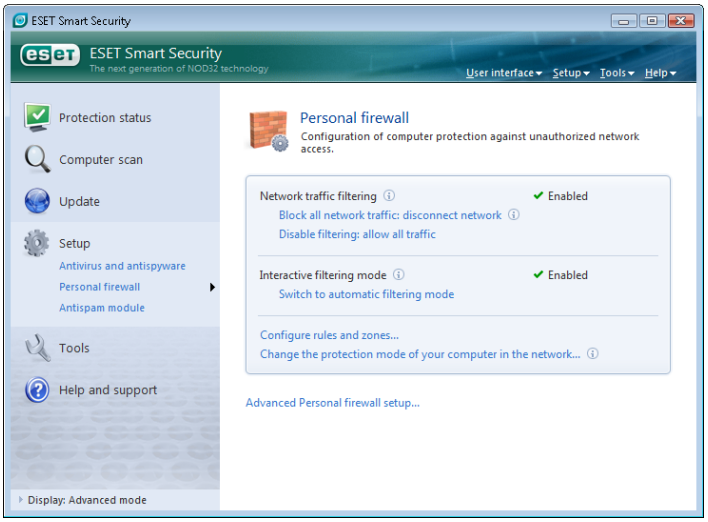
Filtering can be performed in one of the three modes:

- Automatic filtering mode is the default mode. It is suitable for users who prefer easy and convenient use of the firewall with no need to define rules. Automatic mode allows all outbound traffic for the given system and blocks all new connections initiated from the network side.
- Interactive filtering mode allows you to build a tailor-made configuration for your Personal firewall. When a communication is detected and no rule exists which applies to that communication, a dialog window reporting an unknown connection will be displayed. The dialog window gives the option of allowing or denying the communication, and the decision to allow or deny can be remembered as a new rule for the Personal firewall. If the user chooses to create a new rule at this time, all future connections of this type will be allowed or blocked according to the rule.
- Policy-based mode blocks all connections which are not defined by a specific rule that allows them. This mode allows advanced users to define rules that permit only desired and secure connections. All other unspecified connections will be blocked by the Personal firewall.



4.2.2 Block all traffic: disconnect network

The only option for definitively blocking all network traffic is to use the **Block all network traffic: disconnect network** option. Any inbound or outbound communication is blocked by the Personal firewall with no warning displayed. Use this blocking option only if you suspect critical security risks requiring disconnection of the system from the network.



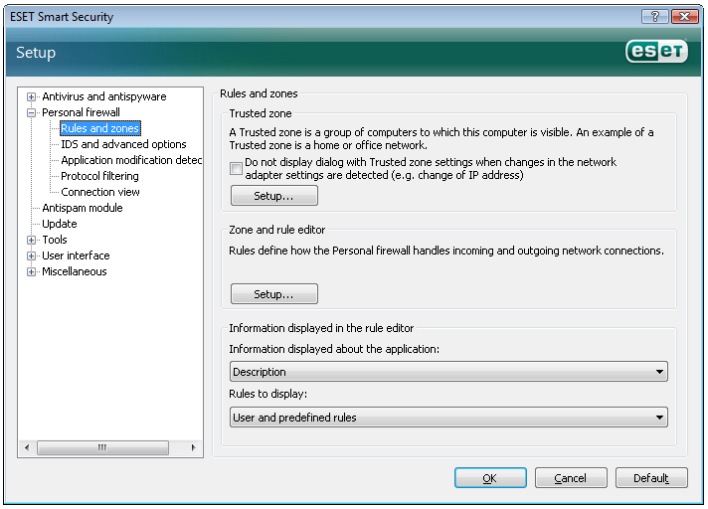
4.2.3 Disable filtering: allow all traffic

The Disable filtering option is the opposite configuration of the above-mentioned blocking of all communication. If selected, all of the Personal firewall's filtering options are turned off and all incoming and outgoing connections are permitted. Where the network is concerned, it has the same effect as no firewall being present.

4.2.4 Configuring and using rules

Rules represent a set of conditions used to meaningfully test all network connections and all actions assigned to these conditions. In Personal firewall, you can define what action to take if a connection defined by a rule is established.

To access the rule filtering setup, navigate to **Advanced setup** (F5) **> Personal firewall > Rules and zones**. To display the current configuration, click **Setup...** in the **Zone and rule editor** section (if the Personal firewall is set to **Automatic filtering mode**, these settings are not available).


ESET Smart Security
Setup
Antivirus and antispyware
Personal firewall
Rules and zones
IDS and advanced options
Application modification detec
Protocol filtering
Connection view
Antispam module
Update
Tools
User interface
Miscellaneous
Rules and zones
Trusted zone
A Trusted zone is a group of computers to which this computer is visible. An example of a Trusted zone is a home or office network.
Do not display dialog with Trusted zone settings when changes in the network adapter settings are detected (e.g. change of IP address)
Setup...
Zone and rule editor
Rules define how the Personal firewall handles incoming and outgoing network connections.
Setup...
Information displayed in the rule editor
Information displayed about the application:
Description
Rules to display:
User and predefined rules
OK
Cancel
Default

In the **Zone and rule setup** window, an overview of either rules or zones is displayed (based on the currently selected tab). The window is divided into two sections. The upper section lists all rules in a

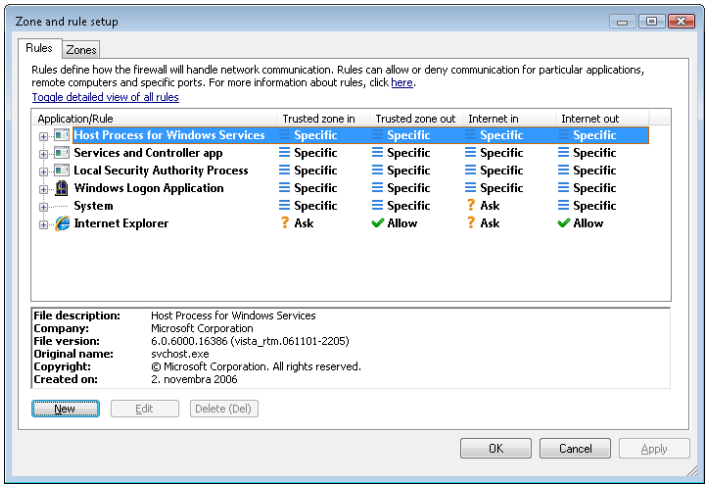
shortened view. The lower section displays details about the rule currently selected in the upper section. At the very bottom are the buttons **New**, **Edit**, and **Delete**, which allow the user to configure rules.

If taking into account the direction of communication, connections can be divided into incoming and outgoing connections. Incoming connections are initiated by a remote computer attempting to establish connection with the local system. Outgoing connections work in the opposite way – the local side contacts a remote computer.

If a new unknown communication is detected, you must carefully consider whether to allow or deny it. Unsolicited, unsecured or totally unknown connections pose a security risk to the system. If such a connection is established, we recommend that you pay particular attention to the remote side and the application attempting to connect to your computer. Many infiltrations try to obtain and send private data, or download other malicious applications to the host workstations. The Personal firewall allows the user to detect and terminate such connections.

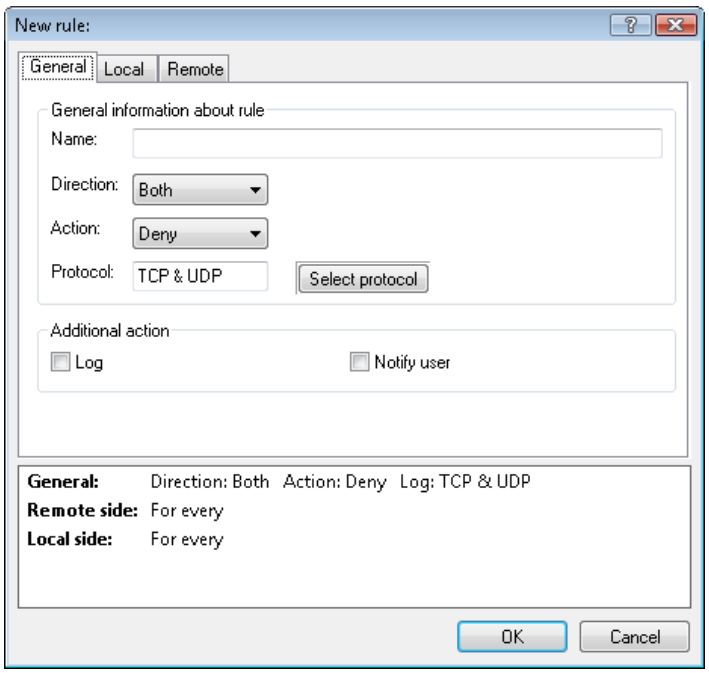
4.2.4.1 Creating new rules

When installing a new application which accesses the network or when modifying an existing connection (remote side, port number, etc.), a new rule must be created.



To add a new rule, verify that the **Rules** tab is selected. Then, click the **New** button in the **Zone and rule** setup window. Clicking on this button opens a new dialog window which allows the specification of a new rule. The upper part of the window contains three tabs:

- **General:** Specifies the name of the rule, direction, action and protocol. Direction is either in or out (or both). Action means allowing or denying the given connection.
- **Local:** Displays information about the local side of the connection, including the number of the local port or port range and the name of the communicating application.
- **Remote:** This tab contains information about the remote port (port range). It also allows the user to define a list of remote IP addresses or zones for a given rule.



A good example of adding a new rule is allowing your Internet browser to access the network. The following must be provided in this case:

- On the **General** tab, enable outgoing communication via the TCP & UDP protocol
- Add the process representing your browser application (for Internet Explorer it is iexplore.exe) on the **Local** tab
- On the **Remote** tab, enable port number 80 only if you wish to allow standard World Wide Web services

4.2.4.2 Editing rules

To modify an existing rule, click the **Edit** button. All the above-mentioned parameters (which are described in the chapter "Creating new rules") can be modified.

Modification is required each time any of the monitored parameters are changed. As a result, the rule does not fulfill the conditions and the specified action cannot be applied. In the end, the given connection may be refused, which can result in problems with operation of the application in question. An example is a change of network address or port number for the remote side.

4.2.5 Configuring zones

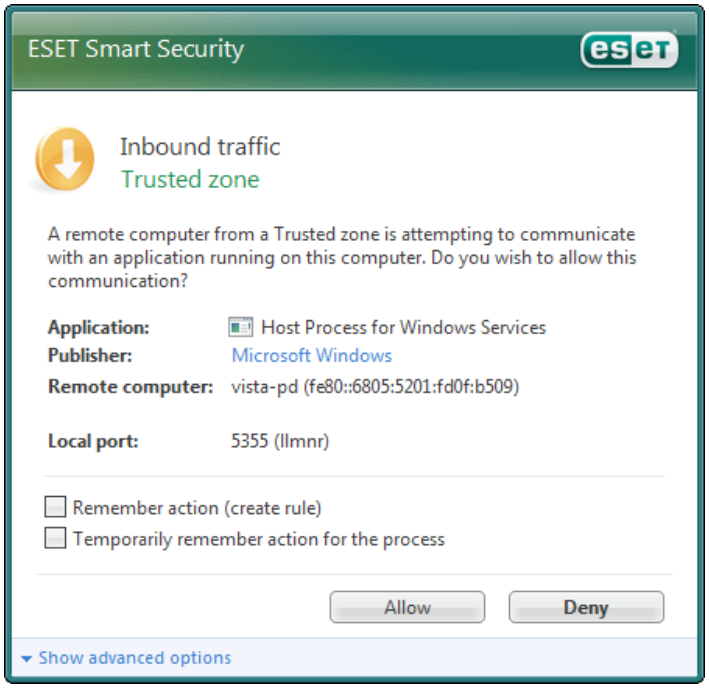
A zone represents a collection of network addresses which create one logical group. Each address in a given group is assigned similar rules defined centrally for the whole group. One example of such a group is the Trusted zone. The Trusted zone represents a group of network addresses which are fully trusted by the user and which are not blocked by the Personal firewall in any way.

These zones can be configured using the **Zones** tab in the **Zone and rule setup** window, by clicking the **New** button. Enter the name of the zone, its description and list of network addresses into the newly opened window.

4.2.6 Establishing connection – detection

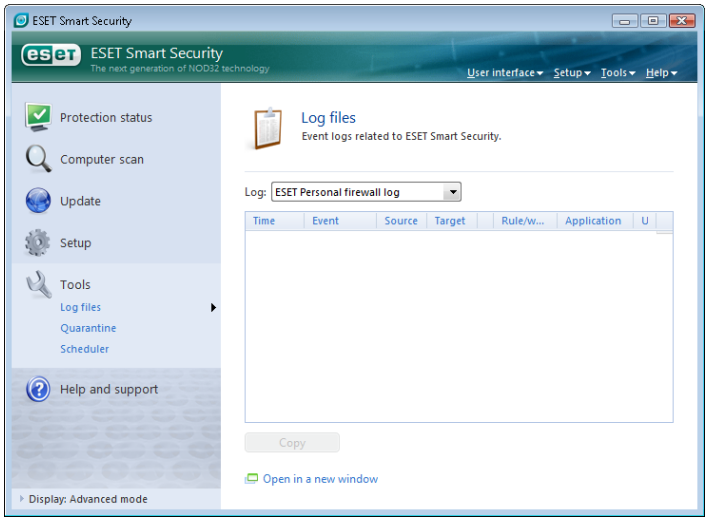
The Personal firewall detects each newly-created network connection. The active firewall mode (Automatic, Interactive, Policy-based) determines which actions are performed for the new rule. Where either the Automatic or Policy-based mode is activated, the Personal firewall will perform predefined actions with no user intervention.

The interactive mode displays an informational window which reports detection of a new network connection, supplemented with detailed information about the connection. The user can opt to allow the connection or refuse (block) it. If you repeatedly allow the same connection in the dialog window, we recommend that you create a new rule for the connection. To do this, select the **Remember action** option (Create rule) and save the action as a new rule for the Personal firewall. If the firewall recognizes the same connection in the future, it will apply the existing rule.


ESET Smart Security
Inbound traffic
Trusted zone
A remote computer from a Trusted zone is attempting to communicate with an application running on this computer. Do you wish to allow this communication?
Application: Host Process for Windows Services
Publisher: Microsoft Windows
Remote computer: vista-pd (fe80::6805:5201:fd0f:b509)
Local port: 5355 (llmnr)
Remember action (create rule)
Temporarily remember action for the process
Allow
Deny
Show advanced options

Please be careful when creating new rules and only allow connections which are secure. If all connections are allowed, then the Personal firewall fails to accomplish its purpose. These are the important parameters for connections:

- **Remote side:** Only allow connections to trusted and known addresses
- **Local application:** It is not advisable to allow connections for unknown applications and processes
- **Port number:** Communication on common ports (e.g. web – port number 80) is usually secure



In order to proliferate, computer infiltrations often use the Internet and hidden connections to help them infect remote systems. If rules are correctly configured, a Personal firewall becomes a useful tool for protection against a variety of malicious code attacks.

4.2.7 Logging

The ESET Smart Security Personal firewall saves all important events in a log file, which can be viewed directly from the main menu. Click **Tools > Log files** and then select **ESET Personal firewall log** from the **Log** drop-down menu.

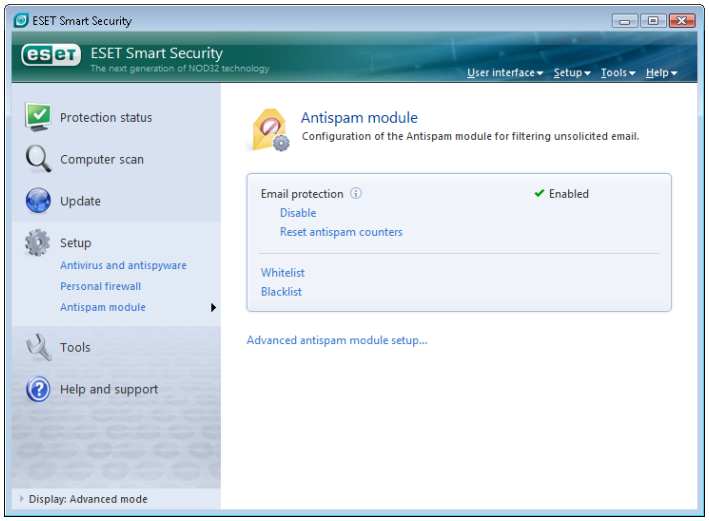
The log files are an invaluable tool for detecting errors and revealing intrusions into the system, and should be given appropriate attention. ESET Personal firewall logs contain the following data:

- Date and time of event
- Name of event
- Source and target network address
- Network communication protocol
- Rule applied, or name of worm, if identified
- Application involved

A thorough analysis of this data can help detect attempts to compromise system security. Many other factors indicate potential security risks and allow the user to minimize their impact: too frequent connections from unknown locations, multiple attempts to establish connections, unknown applications communicating, or unusual port numbers used.

4.3 Antispam protection

Nowadays, unsolicited email – spam – ranks among the greatest problems of electronic communication. It represents up to 80 percent of all email communication. Antispam protection serves to protect against this problem. Combining several very efficient principles, the Antispam module provides superior filtering.



One important principle in spam detection is the ability to recognize unsolicited email based on predefined trusted (whitelist) and spam addresses (blacklist). All addresses from your email client are automatically added to the Whitelist, as well as all other addresses marked by the user as safe.

The primary method used to detect spam is the scanning of email message properties. Received messages are scanned for basic Antispam criteria (message definitions, statistical heuristics, recognizing algorithms and other unique methods) and the resulting index value determines whether a message is spam or not.

The Bayesian filter is also utilized in filtering. By marking messages as *spam* and *not spam*, the user creates a database of words used in each of these respective categories. The larger the database, the more accurate the results it yields.

A combination of the above-mentioned methods provides a high Antispam detection rate.

ESET Smart Security supports Antispam protection for Microsoft Outlook, Outlook Express and Windows Mail.

4.3.1 Self-learning Antispam

Self-learning of Antispam is related to the previously mentioned Bayesian filter. The importance of individual words changes during the "learning" process of marking individual messages as spam or not spam. Accordingly, the more messages that are classified (marked as spam or not spam), the more accurate the results obtained with the Bayesian filter will be.

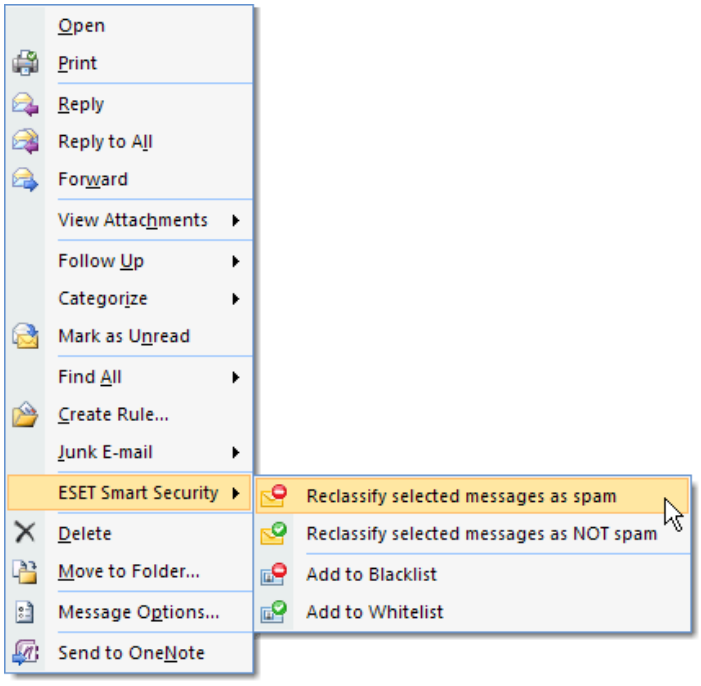
Add known addresses to the whitelist to exclude messages from these addresses from filtering.

4.3.1.1 Adding addresses to Whitelist

Email addresses belonging to people whom the user communicates with frequently can be added to the list of "safe" addresses (Whitelist). Doing so ensures that no message originating from a whitelist address is ever classified as spam. To add a new address to the whitelist, right-click on the given email message and select **Add to Whitelist** under the ESET Smart Security context menu option, or click **Trusted address** in the ESET Smart Security Antispam toolbar in the upper section of your email program. Similarly, this process applies to spam addresses. If an email address is listed on the blacklist, each email message which arrives from that address is classified as spam.

4.3.1.2 Marking messages as spam

Any message viewed in your email client can be marked as spam. To do so, use the context menu (right-click) and then click **ESET Smart Security > Reclassify selected messages as spam**) or click **Spam** from the ESET Smart Security Antispam toolbar located in your email client.



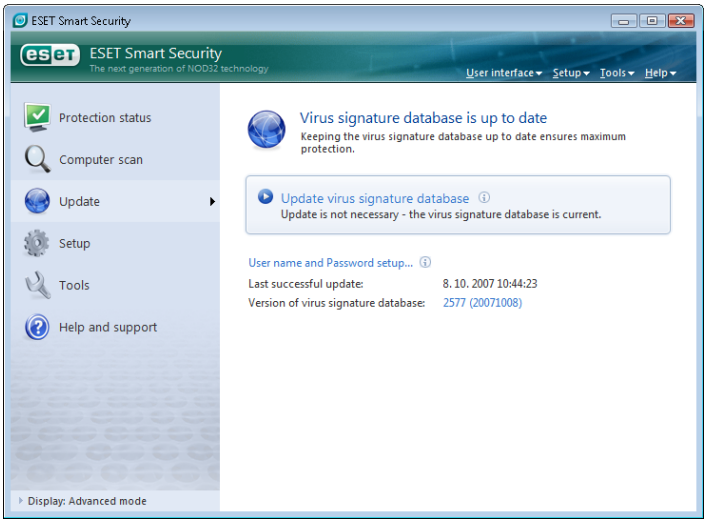
Reclassified messages are automatically moved to the SPAM folder, but the sender email address is not added to blacklist. Similarly, messages can be classified as "not spam". If messages from the **Junk E-mail** folder are classified as not spam, they are moved to their original folder. Marking a message as not spam does not automatically add the sender address to the Whitelist.

4.4 Updating the program

Regular updating of the system is the basic premise for obtaining the maximum level of security provided by ESET Smart Security. The Update module ensures that the program is always up to date. This is done in two ways – by updating the virus signature database and by updating all system components.

Information about the current update status can be found by clicking **Update**, including the current version of the virus signature database and whether an update is required. In addition, the option to activate the update process immediately – **Update virus signature database** – is available, as well as basic update setup options such as the user name and password to access ESET's update servers.

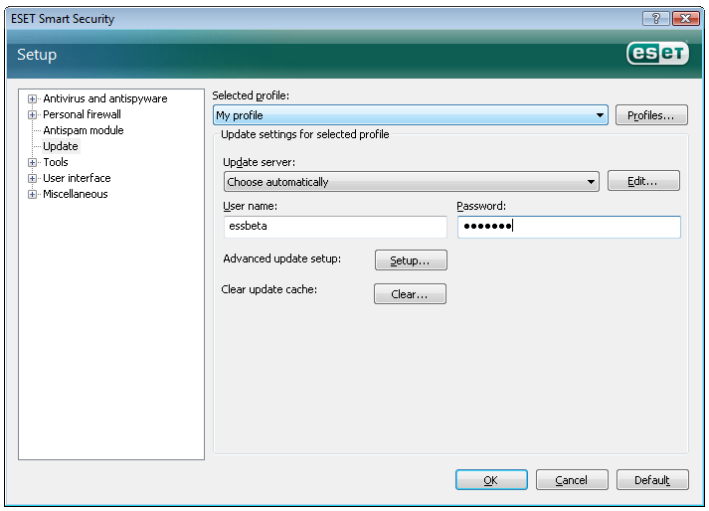
The information window also contains details such as the date and time of the last successful update and the number of the virus signature database. This numeric indication is an active link to ESET's web site, listing all signatures added within the given update.



NOTE: The User name and Password is provided by ESET after purchase of ESET Smart Security.

4.4.1 Update setup

The update setup section specifies the update source information, such as the update servers and authentication data for these servers. By default, the **Update server:** field is set to **Choose automatically**. This value ensures that the update files will automatically be downloaded from the ESET server with the least network traffic load. The update setup options are available from the Advanced Setup (F5) tree, under **Update**.



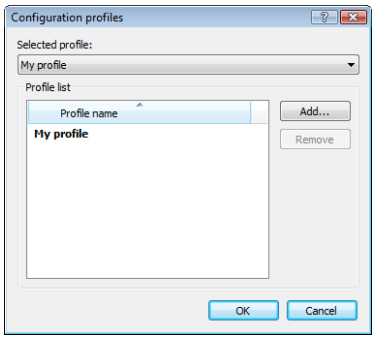
The list of currently existing update servers is accessible via the **Update server:** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

Authentication for update servers is granted by the **User name** and **Password** which were generated and sent to the user by ESET after purchase of the product license.

4.4.1.1 Update profiles

For various update configurations, it is possible to create user-defined update profiles which can be used for a given update task. Creating various update profiles is especially useful for mobile users, as the Internet connection properties regularly change. By modifying the update task, mobile users can specify that if it is not possible to update the program using the configuration specified in **My Profile**, the update will be performed using an alternative profile.

The **Selected profile** drop-down menu displays the currently selected profile. By default, this entry is set to **My profile**. To create a new profile, click the **Profiles...** button and then click the **Add...** button and enter your own **Profile name**. When creating a new profile, you can copy settings from an existing one by selecting it from the **Copy settings from profile:** drop-down menu.



Within the profile setup, you can specify the update server to which the program will connect and download updates; any server from the list of available servers can be used, or a new server can be added. The list of existing update servers is accessible via the **Update server:** drop-down menu. To add a new update server, click **Edit...** in the **Update settings for selected profile** section and then click the **Add** button.

4.4.1.2 Advanced update setup

To view the **Advanced update setup**, click the **Setup...** button. Advanced update setup options include configuration of **Update Mode, HTTP Proxy, LAN** and **Mirror**.

4.4.1.2.1 Update mode

The **Update mode** tab contains options related to the program component update.

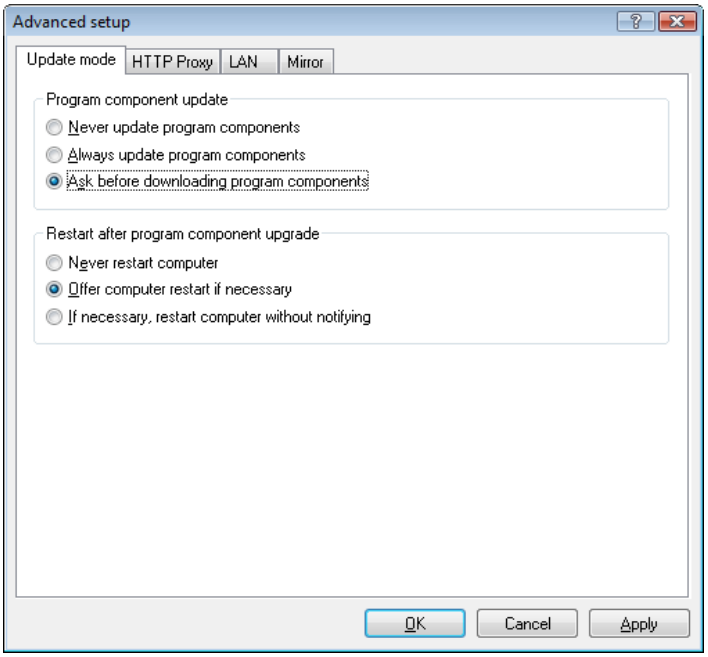
In the **Program component update** section, three options are available:

- **Never update program components**
- **Always update program components**
- **Ask before downloading program components**

Selecting the option **Never update program components** ensures that after a new program component update has been issued by ESET, it will not be downloaded and no program component update will actually take place on the given workstation. The **Always update program components** option means that program component updates will be performed each time a new update is available on ESET's update servers, and that program components will be upgraded to the downloaded version.

Select the third option, **Ask before downloading program components** to ensure that the program will ask the user to confirm downloading of program component updates at the moment such updates are available. In this case, a dialog window containing information about the available program component updates will be displayed, with the option to confirm or refuse it. If confirmed, updates are downloaded and new program components will be installed.

The default option for a program components update is **Ask before downloading program components**.



After installation of a program component update, it is necessary to restart the system in order to provide full functionality of all modules. The section **Restart after program component upgrade** allows you to select one of the following three options:

- **Never restart computer**
- **Offer computer restart if necessary**
- **If necessary, restart computer without notifying**

The default option for restarting is **Offer computer restart if necessary**. Selection of the most appropriate options for program

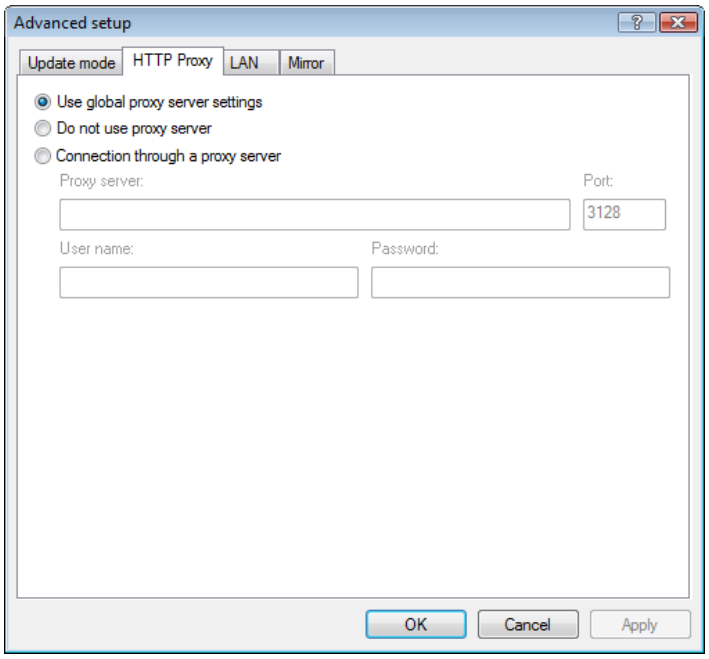
component updates within the **Update mode** tab depends on each individual workstation, since that is where these settings are to be applied. Please be aware that there are differences between workstations and servers – e.g. restarting the server automatically after a program upgrade could cause serious damage.

4.4.1.2.2 Proxy server

To access the proxy server setup options for a given update profile: Click **Update** in the Advanced Setup tree (F5) and then click the **Setup...** button to the right of **Advanced update setup.** Click the **HTTP Proxy** tab and select one of the three following options:

- **Use global proxy server settings**
- **Do not use proxy server**
- **Connection through a proxy server** (connection defined by the connection properties)

Selecting the **Use global proxy server settings** option will use the proxy server configuration options already specified within the **Miscellaneous > Proxy server** branch of the Advanced Setup tree.



Select the **Do not use proxy server** option to explicitly define that no proxy server will be used for updating ESET Smart Security.

The **Connection through a proxy server** option should be chosen if a proxy server is to be used for updating ESET Smart Security and is different from the proxy server specified in the global settings (**Miscellaneous > Proxy server**). If so, the settings should be specified here: **Proxy server** address, communication **Port**, plus **User name** and **Password** for the proxy server if required.

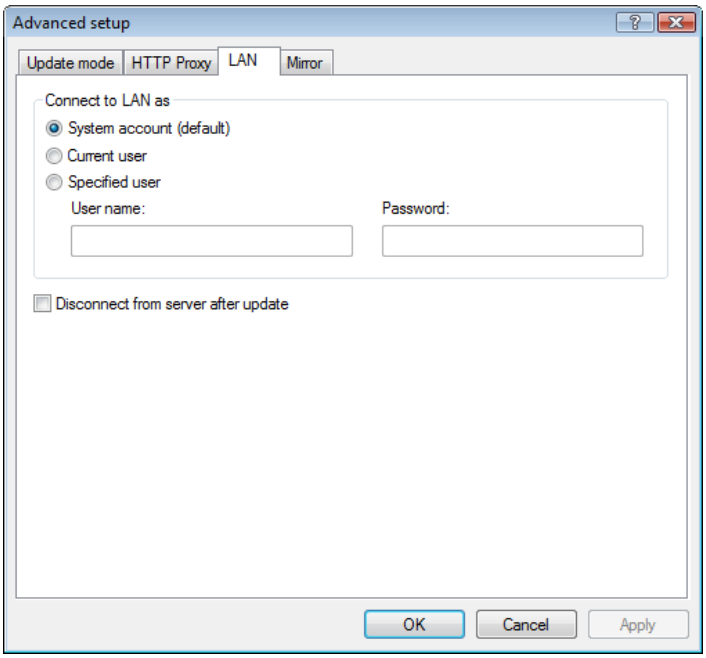
This option should also be selected if the proxy server settings were not set globally, but the ESET Smart Security will connect to a proxy server for updates.

The default setting for the proxy server is **Use global proxy server settings**.

4.4.1.2.3 Connecting to LAN

When updating from a local server with an NT-based operating system, authentication for each network connection is required by default. In most cases, a local system account doesn't have sufficient rights to access the Mirror folder (the Mirror folder contains copies of update files). If this is the case, enter the user name and password in the update setup section, or specify an existing account under which the program will enter the update server (Mirror).

To configure such an account, click the **LAN** tab. The **Connect to LAN as** section offers the options **System account (default)**, **Current user**, and **Specified user**.



Select the **System account** option to use the system account for authentication. Normally, no authentication process takes place if there is no authentication data supplied in the main update setup section.

To ensure that the program authorizes itself using a currently logged-in user account, select **Current user**. The drawback of this solution is that the program is not able to connect to the update server if no user is currently logged in.

Select **Specified user** if you want the program to use a specific user account for authentication.

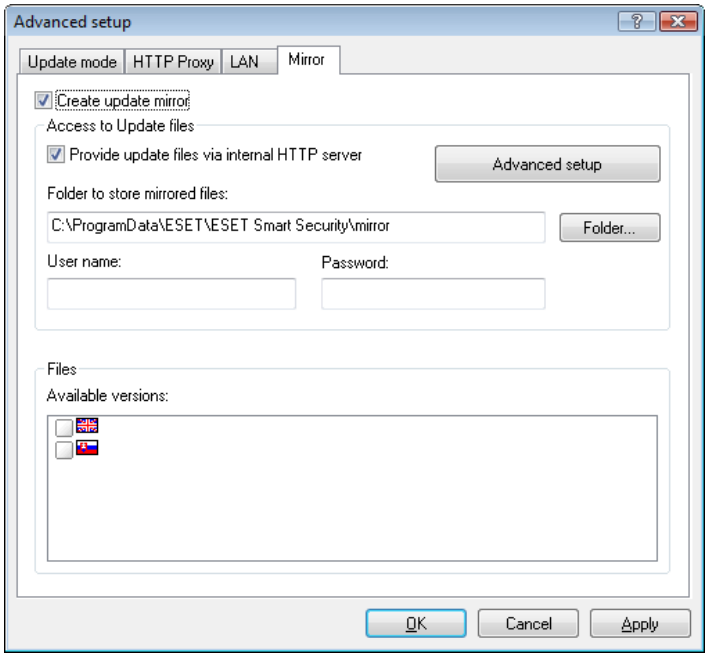
The default option for LAN connection is **System account**.

Warning:
When either **Current user** or **Specified user** is enabled, an error may occur when changing the identity of the program to the desired user. This is why we recommend inserting the LAN authentication data in the main update setup section. In this update setup section, the authentication data should be entered as follows: domain_name\user (if it is a workgroup, enter workgroup_name\name) and the user's password. When updating from the HTTP version of the local server, no authentication is required.

4.4.1.2.4 Creating update copies – Mirror

ESET Smart Security Business Edition allows the user to create copies of update files which can be used to update other workstations located in the network. Updating client workstations from a Mirror optimizes network load balance and saves Internet connection bandwidth.

Configuration options for the local server Mirror are accessible in the **Advanced update setup:** section (to access this section, press F5 and click **Update** in the Advanced Setup tree. Click the **Setup...** button next to **Advanced update setup:** and select the **Mirror** tab).



The first step in configuring the Mirror is to select the **Create update mirror** check box. Selecting this option activates other Mirror configuration options such as the way update files will be accessed and the update path to the mirrored files.

The methods of Mirror activation are described in detail in the next chapter, "Variants of accessing the Mirror". For now, note that there are two basic variants of accessing the Mirror – the folder with update files can be presented as a Mirror as a shared network folder, or a Mirror as an HTTP server.

The folder dedicated to storing update files for the Mirror is defined in the **Folder to store mirrored files** section. Click **Folder...** to browse for a desired folder on the local computer or shared network folder. If authorization for the specified folder is required, authentication data must be supplied in the **User name** and **Password** fields. The User name and Password should be entered in the format *Domain/User* or *Workgroup/User*. Please remember to supply the corresponding passwords.

When specifying detail Mirror configuration, you can also specify the language versions for which you want to download update copies. Language version setup is accessible in the section **Files - Available versions:**.

4.4.1.2.4.1 Updating from the Mirror

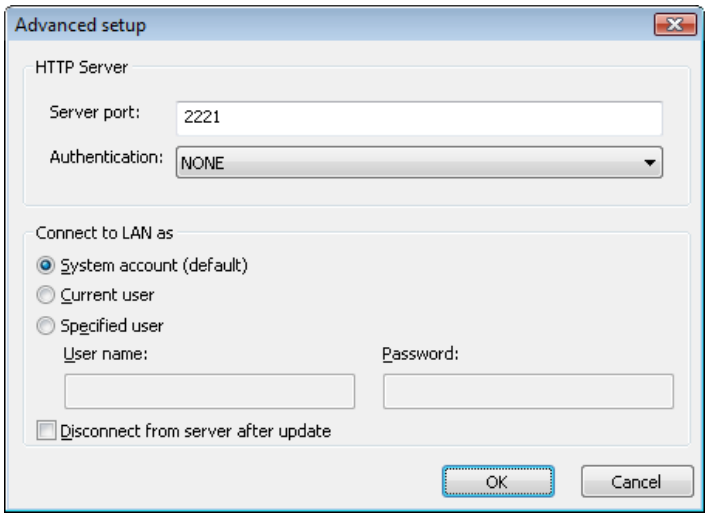
There are two basic methods of configuring the Mirror – the folder with update files can be presented as the Mirror as a shared network folder, or the Mirror as an HTTP server.

Accessing the Mirror using an internal HTTP server

This configuration is the default, specified in the predefined program configuration. In order to allow access to the Mirror using the HTTP server, navigate to **Advance update setup** (the **Mirror** tab) and select the **Create update mirror** option.

In the **Advanced setup** section of the **Mirror** tab you can specify the **Server Port** where the HTTP server will listen as well as the type of **Authentication** used by the HTTP server. By default, the Server port is set to the value **2221**. The **Authentication** option defines the method of authentication used for accessing the update files. The following options are available: **NONE, Basic,** and **NTLM**. Select **Basic** to use the base64 encoding with basic user name and password authentication. The **NTLM** option provides encoding using a safe encoding method. For authentication, the user created on the workstation sharing the update files is used. The default setting is **NONE**, which grants access to the update files with no need for authentication.

Warning:
If you want to allow access to the update files via the HTTP server, the Mirror folder must be located on the same computer as the ESET Smart Security instance creating it.



After configuration of the Mirror is finished, go to the workstations and add a new update server in the format **http://IP_address_of_your_server:2221**. To do this, follow the steps below:

- Open **ESET Smart Security Advanced Setup** and click the **Update** branch.
- Click **Edit...** to the right of the **Update server** drop-down menu and add a new server using the following format: http://IP_address_of_your_server:2221
- Select this newly-added server from the list of update servers.

Accessing the Mirror via system shares

First, a shared folder should be created on a local or a network device. When creating the folder for the Mirror, it is necessary to provide "write" access for the user who will save update files to the folder and "read" access for all users who will update ESET Smart Security from the Mirror folder.

Next, configure access to the Mirror in the **Advanced update setup** section (the **Mirror** tab) by disabling the **Provide update files via internal HTTP server** option. This option is enabled by default in the program install package.

If the shared folder is located on another computer in the network, you must specify authentication data in order to access the other computer. In order to specify authentication data, open ESET Smart Security Advanced Setup (F5) and click the **Update** branch. Click the **Setup...** button and then click the **LAN** tab. This setting is the same as for updating, as described in the chapter"Connecting to LAN".

After the Mirror configuration is complete, proceed to the workstations and set \\UNC\PATH as the update server. This operation can be completed using the following steps:

- Open ESET Smart Security Advanced Setup and click **Update**
- Click **Edit...** next to the Update server and add a new server using the \\UNC\PATH format.

- Select this newly-added server from the list of update servers

NOTE:
For proper functioning, the path to the Mirror folder must be specified as a UNC path. Updates from mapped drives may not work.

4.4.1.2.4.2 Troubleshooting Mirror update problems

Depending on the method used to access the Mirror folder, various types of problems may occur. In most cases, problems during an update from a Mirror server are caused by one or more of the following: incorrect specification of the Mirror folder options, incorrect authentication data to the Mirror folder, incorrect configuration on local workstations attempting to download update files from the Mirror, or by a combination of the reasons above. Here we give an overview of the most frequent problems which may occur during an update from the Mirror:

- **ESET Smart Security reports an error connecting to Mirror server** – likely caused by incorrect specification of the update server (network path to the Mirror folder) from which local workstations download updates. To verify the folder, click the Windows **Start menu**, click **Run**, insert the folder name and click **OK**. The contents of the folder should be displayed.

- **ESET Smart Security requires a user name and password** – likely caused by incorrect entry of authentication data (User name and Password) in the update section. The User name and Password are used to grant access to the update server, from which the program will update itself. Make sure that the authentication data is correct and entered in the correct format. For example, *Domain/User name*, or *Workgroup/User name*, plus the corresponding Passwords. If the Mirror server is accessible to "Everyone", please be aware that this does not mean that just any user is granted access. "Everyone" does not mean any unauthorized user, it just means that that the folder is accessible for all domain users. As a result, if the folder is accessible to "Everyone", a domain user name and password will still need to be entered in the update setup section.

- **ESET Smart Security reports an error connecting to the Mirror server** –communication on the port defined for accessing the HTTP version of the Mirror is blocked.

4.4.2 How to create update tasks

Updates can be triggered manually by clicking **Update virus signature database** in the information window displayed after clicking **Update** from the main menu**.**

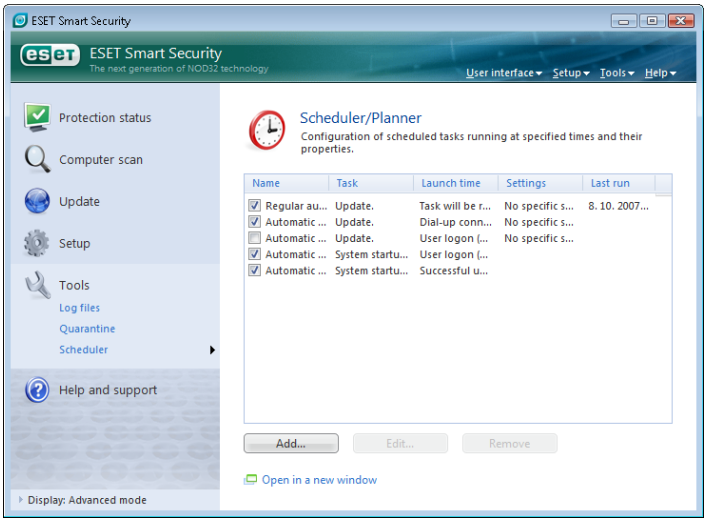
Updates can also be run as scheduled tasks – To configure a scheduled task, click **Tools > Scheduler**. By default, the following tasks are activated in ESET Smart Security:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**

Each of the aforementioned update tasks can be modified to meet your needs. In addition to the default update tasks, you can create new update tasks with a user-defined configuration. For more details about creating and configuring update tasks, see the chapter "Scheduler".

4.5 Scheduler

Scheduler is available if the Advanced mode in ESET Smart Security is activated. **Scheduler** can be found in the ESET Smart Security main menu under **Tools**. Scheduler contains a summary list of all scheduled tasks and their configuration properties such as the predefined date, time, and scanning profile used.



By default, the following scheduled tasks are displayed in **Scheduler**:

- **Regular automatic update**
- **Automatic update after dial-up connection**
- **Automatic update after user logon**
- **Automatic startup file check after user logon**
- **Automatic startup file check after successful update of the virus signature database**

To edit the configuration of an existing scheduled task (both default and user-defined), right-click on the task and click **Edit...** or select the desired task you wish to modify and click the **Edit...** button.

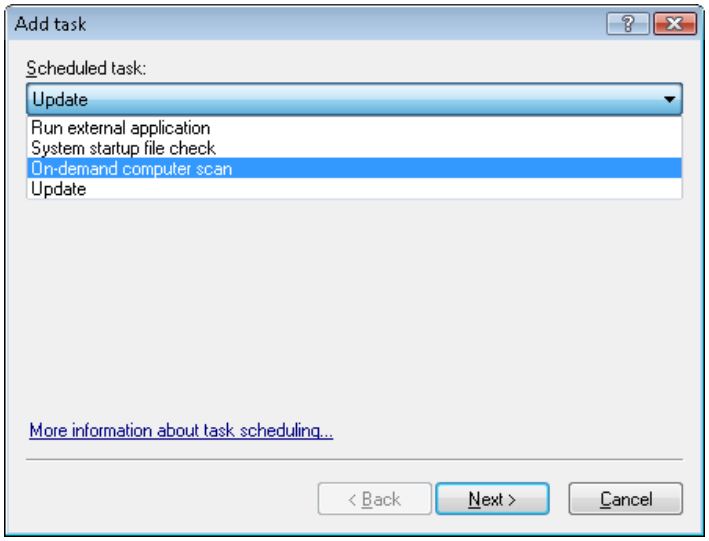
4.5.1 Purpose of scheduling tasks

Scheduler manages and launches scheduled tasks with predefined configuration and properties. The configuration and properties contain information such as the date and time as well as specified profiles to be used during execution of the task.

4.5.2 Creating new tasks

To create a new task in Scheduler, click the **Add...** button or right-click and select **Add...** from the context menu. Five types of scheduled tasks are available:

- **Run external application**
- **Log maintenance**
- **System startup file check**
- **On-demand computer scan**
- **Update**



Since **On-demand computer scan** and **Update** are the most frequently used scheduled tasks, we will explain how to add a new update task.

From the **Scheduled task:** drop-down menu, select **Update**. Click **Next** and enter the name of the task into the **Task name:** field. Select the frequency of the task. The following options are available: **Once, Repeatedly, Daily**, **Weekly** and **Event-triggered**. Based on the frequency selected, you will be prompted with different update parameters. Next, define what action to take if the task cannot be performed or completed at the scheduled time. The following three options are available:

- **Wait until the next scheduled time**
- **Run task as soon as possible**
- **Run task immediately if the time since its last execution exceeds specified interval** (the interval can be defined immediately using the **Task interval** scroll box)

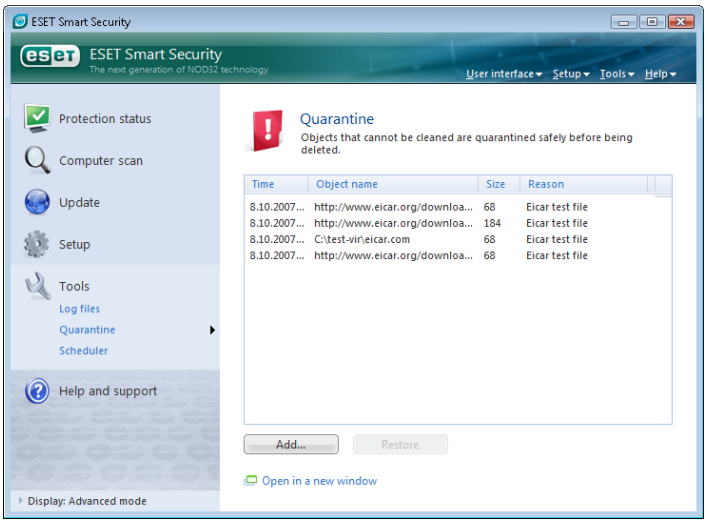
In the next step, a summary window with information about the current scheduled task is displayed; the option **Run task with specific parameters** should be automatically enabled. Click the **Finish** button.

A dialog window will appear, allowing you to select profiles to be used for the scheduled task. Here you can specify a primary and alternative profile, which is used in case the task cannot be completed using the primary profile. Confirm by clicking **OK** in the **Update profiles** window. The new scheduled task will be added to the list of currently scheduled tasks.

4.6 Quarantine

The main task of quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them, or if they are being falsely detected by ESET Smart Security.

The user can choose to quarantine any file he or she wants to. This is advisable if a file behaves suspiciously but is not detected by the antivirus scanner. Quarantined files can be submitted for analysis to ESET's virus laboratories.



Files stored in the quarantine folder can be viewed in a table which displays the date and time of quarantine, the path to the original location of the infected file, its size in bytes, reason (**added by user...**), and number of threats (e.g., if it is an archive containing multiple infiltrations).

4.6.1 Quarantining files

The program automatically quarantines deleted files (if you have not cancelled this option in the alert window). If desired, you can quarantine any suspicious file manually by clicking the **Add...** button. If this is the case, the original file is not removed from its original location. The context menu can also be used for this purpose – right-click in the quarantine window and select **Add...**

4.6.2 Restoring from Quarantine

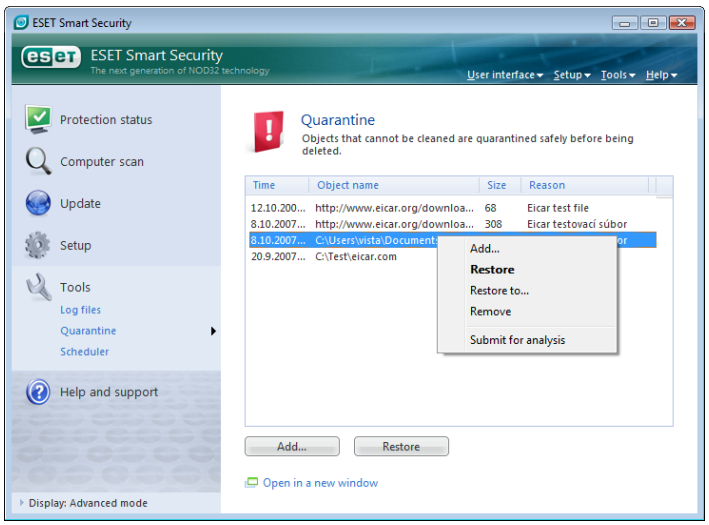
Quarantined files can also be restored to their original location. Use the **Restore** feature for this purpose; this is available from the context menu by right-clicking on the given file in the quarantine window. The context menu also offers the option **Restore to**, which allows you to restore a file to a location other than the one from which it was deleted.

NOTE:
If the program quarantined a harmless file by mistake, please exclude the file from scanning after restoring and send the file to ESET Customer Care.

4.6.3 Submitting file from Quarantine

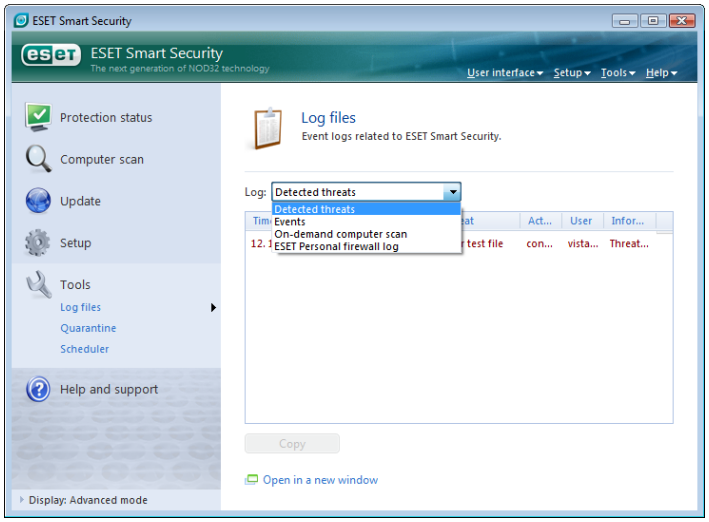
If you have quarantined a suspicious file that was not detected by the program, or if a file was incorrectly evaluated as infected (e.g. by heuristic analysis of the code) and subsequently quarantined, please

send the file to ESET's virus lab. To submit a file from quarantine, right-click the file and select **Submit for analysis** from the context menu.



4.7 Log files

The Logs files contain information about all important program events that have occurred and provide an overview of detected threats. Logging acts as an essential tool in system analysis, threat detection and troubleshooting. Logging is performed actively in the background with no user interaction. Information is recorded based on the current log verbosity settings. It is possible to view text messages and logs directly from the ESET Smart Security environment, as well as to archive logs.



Log files are accessible from the main ESET Smart Security window by clicking **Tools > Log files**. Select the desired log type using the **Log:** drop-down menu at the top of the window. The following logs are available:

1. **Detected threats** – Use this option to view all information about events related to the detection of infiltrations.

2. **Events** – This option is designed for system administrators and users to solve problems. All important actions performed by ESET Smart Security are recorded in the Event logs.

3. **On-demand computer scan** – Results of all completed scans are displayed in this window. Double-click on any entry to view details of the respective On-demand scan.

4. **ESET Personal firewall log** – Contains records of all facts detected by and related to the Personal firewall. Analysis of the firewall log may help to detect system penetration attempts in time to prevent unauthorized access to your system.

In each section, the displayed information can be directly copied to the clipboard by selecting the entry and clicking the **Copy** button. To select multiple entries, the CTRL and SHIFT keys can be used.

4.7.1 Log maintenance

The Logging configuration of ESET Smart Security is accessible from the main program window. Click **Setup > Enter entire advanced setup tree... > Tools > Log files**. You can specify the following options for log files:

- **Delete records automatically:** Log entries older than the specified number of days are automatically deleted

- **Optimize log files automatically**: Enables automatic defragmentation of log files if the specified percentage of unused records has been exceeded

- **Minimum logging verbosity:** Specifies the logging verbosity level. Available options:

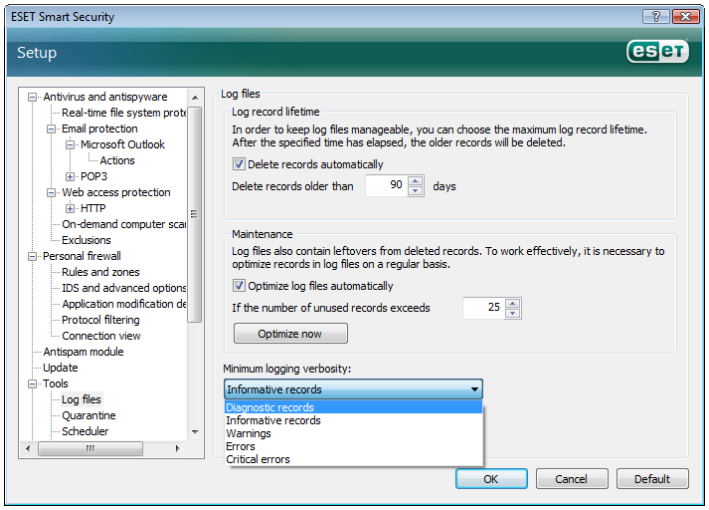
  - **Critical errors** – Logs only critical errors (error starting Antivirus protection, Personal firewall, etc...)

  - **Errors** – Only "Error downloading file" messages are recorded, plus critical errors

  - **Warnings** – Records critical errors and warning messages

  - **Informative records** – Records informative messages including successful update messages plus all records above

  - **Diagnostic records** – Logs information needed for fine-tuning of the program and all records above



4.8 User interface

The user interface configuration options in ESET Smart Security can be modified so that you can adjust the working environment to fit your needs. These configuration options are accessible from the **User interface** branch of the ESET Smart Security Advanced Setup tree.

The **User interface elements** section gives users the ability to toggle to Advanced mode if desired. Advanced mode displays more detailed settings and additional controls to ESET Smart Security.

The **Graphical user interface** option should be disabled if the graphical elements slow the performance of the computer, or cause other problems. The graphical interface may also need to be turned off

for visually impaired users, as it may conflict with special applications that are used for reading text displayed on the screen.

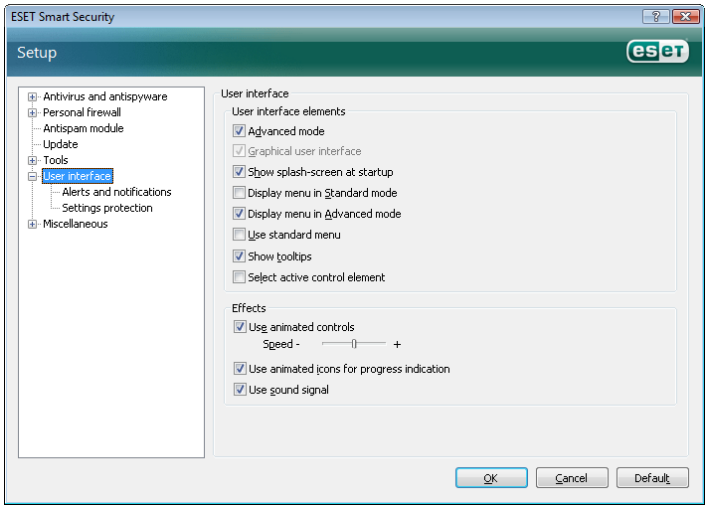
If you wish to deactivate the ESET Smart Security splash-screen, disable the **Show splash-screen at startup** option.

At the top of the ESET Smart Security main program window, there is a Standard menu which can be activated or disabled based on the **Use standard menu** option.

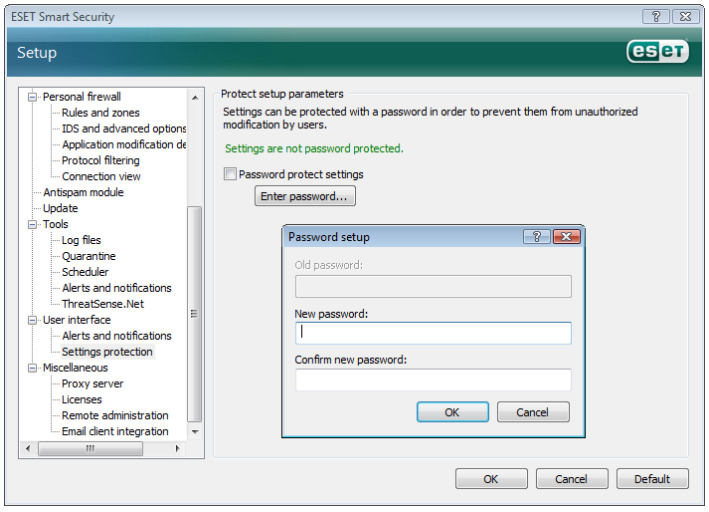
If the **Show tooltips** option is enabled, a short description of any option will be displayed if the cursor is placed over the option. The **Select active control element** option will cause the system to highlight any element which is currently under the active area of the mouse cursor. The highlighted element will be activated after a mouse click.

To decrease or increase the speed of animated effects, select the **Use animated controls** option and move the **Speed** slider bar to the left or right.

To enable the use of animated icons to display the progress of various operations, select the **Use animated icons...** check box.If you want the program to sound a warning if an important event takes place, select the **Use sound signal** option.



The **User interface** features also include the option to password-protect the ESET Smart Security setup parameters. This option is located in the **Settings protection** submenu under **User interface**. In order to provide maximum security for your system, it is essential that the program be correctly configured. Unauthorized modifications could result in the loss of important data. To set a password to protect the setup parameter, click **Enter password...**



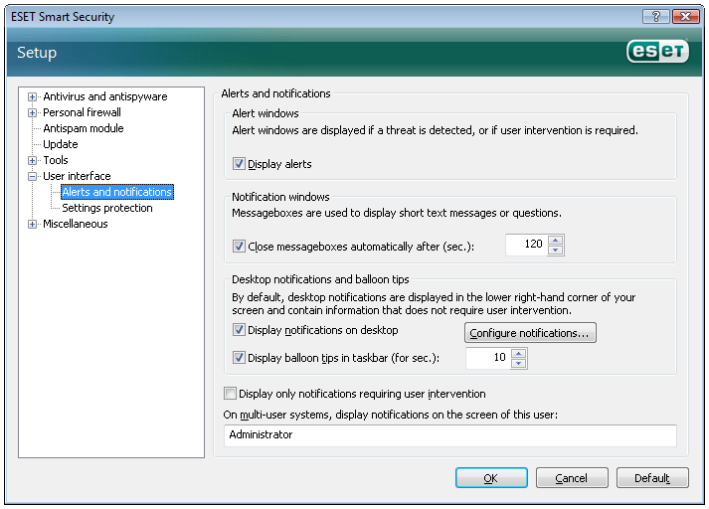
4.8.1 Alerts and notifications

The **Alerts and notifications setup** section under **User interface** allows you to configure how threat alert messages and system notifications are handled in ESET Smart Security.

The first item is **Display alerts**. Disabling this option will cancel all alert windows and is only suitable for a limited amount of specific situations. For most users, we recommend that this option be left to its default setting (enabled).

To close pop-up windows automatically after a certain period of time, select the option **Close messageboxes automatically after (sec.)**. If they are not closed manually by the user, alert windows are automatically closed after the specified time period has expired.

Notifications on the desktop and balloon tips are informative only, and do not require or offer user interaction. They are displayed in the notification area at the bottom right corner of the screen. To activate displaying desktop notifications, select the **Display notifications on desktop** option. More detailed options – notification display time and window transparency can be modified by clicking the **Configure notifications...** button. To preview the behavior of notifications, click the **Preview** button. To configure the duration of the balloon tips display time, see the option **Display balloon tips in taskbar (for sec.)**.


ESET Smart Security
Setup
Antivirus and antispyware
Personal firewall
Antispam module
Update
Tools
User interface
Alerts and notifications
Settings protection
Miscellaneous
Alerts and notifications
Alert windows
Alert windows are displayed if a threat is detected, or if user intervention is required.
Display alerts
Notification windows
Messageboxes are used to display short text messages or questions.
Close messageboxes automatically after (sec.):
120
Desktop notifications and balloon tips
By default, desktop notifications are displayed in the lower right-hand corner of your screen and contain information that does not require user intervention.
Display notifications on desktop
Configure notifications...
Display balloon tips in taskbar (for sec.):
10
Display only notifications requiring user intervention
On multi-user systems, display notifications on the screen of this user:
Administrator
OK
Cancel
Default

In the bottom section of the **Alerts and notifications** setup window, there is the option **Display only notifications requiring user intervention**. This option allows you to turn on/off displaying of alerts and notifications that require no user intervention. The last feature of this section is specifying addresses of notifications in a multi-user environment.

The **On multi-user systems, display notifications on the screen of the user**: field allows the user to define who will receive important notifications from ESET Smart Security. Normally this would be a system or network administrator. This option is especially useful for terminal servers, provided that all system notifications are sent to the administrator.

4.9 ThreatSense.Net

The ThreatSense.Net Early Warning System is a tool that keeps ESET immediately and continuously informed about new infiltrations. The bidirectional ThreatSense.Net Early Warning System has a single purpose – to improve the protection that we can offer you. The best way to ensure that we see new threats as soon as they appear is to "link" to as many of our customers as possible and use them as our Threat Scouts. There are two options:

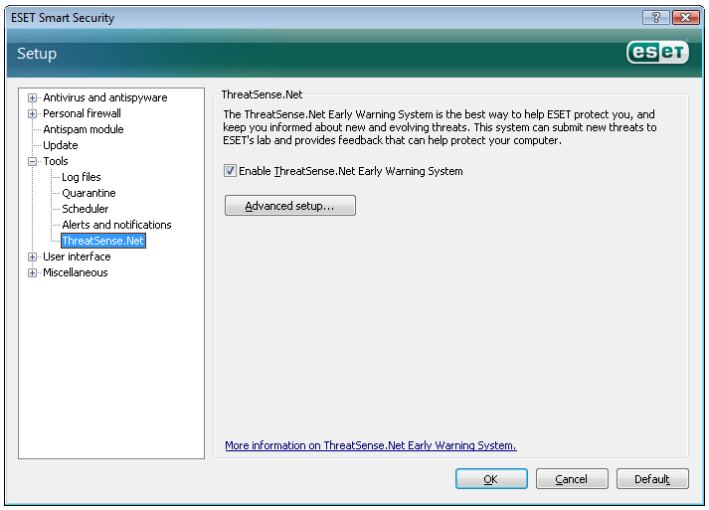
- You can decide not to enable the ThreatSense.Net Early Warning System. You won't lose any functionality in the software, and you'll still get the best protection that we can offer.

- You can configure the Early Warning System to submit anonymous information about new threats and where the new threatening code is contained, in a single file. This file can be sent to ESET for detailed analysis. Studying these threats will help ESET update its threat detection capabilities. The ThreatSense.Net Early Warning System will collect information about your computer related to newly-detected threats. This information may include a sample or copy of the file in which the threat appeared, the path to that file, the file name, information about the date and time, the process by which the threat appeared on your computer and information about your computer's operating system. Some of this information may include personal information about the user of the computer, such as user names in a directory path, etc.

While there is a chance that this may occasionally disclose some information about you or your computer to our threat lab at ESET, this information will not be used for ANY purpose other than to help us respond immediately to new threats.

By default, ESET Smart Security is configured to ask before submitting suspicious files for detailed analysis to ESET's threat lab. It should be noted that files with certain extensions such as .doc or .xls are always excluded from sending, should a threat be detected in them. You can also add other extensions if there are particular files that you or your organization wants to avoid sending.

The ThreatSense.Net setup is accessible from the Advanced Setup tree, under **Tools > ThreatSense.Net**. Select the **Enable ThreatSense.Net Early Warning System** check box. This will allow you to activate and then click the **Advanced Setup...** button.

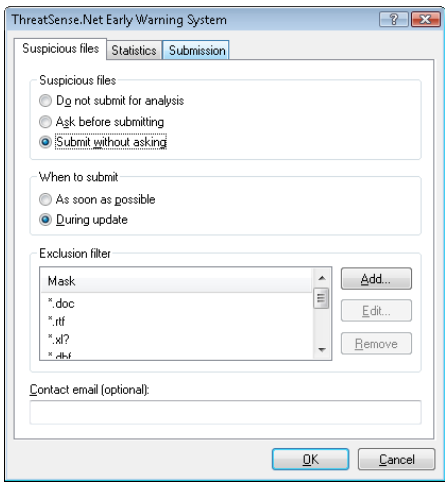


4.9.1 Suspicious files

The **Suspicious files** tab allows you to configure the manner in which threats are submitted to ESET's lab for analysis.

If you have found a suspicious file, you can submit it for analysis to our virus labs. If it turns out to be a malicious application, its detection will be added to the next virus signature update.

Submission of files can be set to be performed automatically without asking. If this option is selected, suspicious files are sent in the background. If you wish to know which files have been sent for analysis and confirm the submission, select the **Ask before submitting** option.



If you don't want any files to be submitted, select **Do not submit for analysis**. Note that not submitting files for analysis does not affect submission of statistical information to ESET. Statistical information is configured in its own setup section, described in the next chapter.

When to submit
Suspicious files will be sent to ESET's labs for analysis as soon as possible. This is recommended if a permanent Internet connection is available and suspicious files can be delivered without delay. The other option is to submit suspicious files **During update**. If this option is selected, suspicious files will be collected and uploaded to the Early Warning System servers during an update.

Exclusion filter
Not all files have to be submitted for analysis. The Exclusion filter allows you to exclude certain files/folders from submission. For example, it may be useful to exclude files which may carry potentially confidential information, such as documents or spreadsheets. The most common file types are excluded by default (Microsoft Office, OpenOffice). The list of excluded files can be expanded if desired.

Contact email
The contact email is sent along with suspicious files to ESET and may be used to contact you if further information about submitted files is required for analysis. Please note that you will not receive a response from ESET unless more information is required.

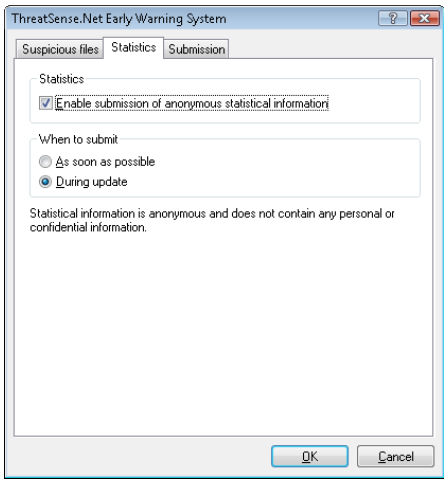
4.9.2 Statistics

The ThreatSense.Net Early Warning System collects anonymous information about your computer which is related to newly detected threats. This information may include the name of the infiltration, the date and time it was detected, the ESET Smart Security version, your computer's operating system version and the location setting. The statistics are normally delivered to ESET's servers once or twice a day.

An example of a statistical package submitted:

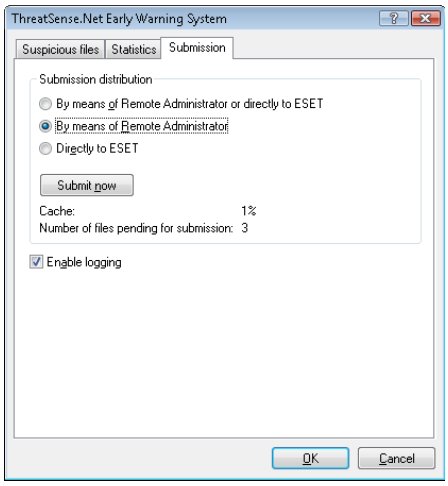
```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

When to submit
In the **When to submit** section, you can define when the statistical info will be submitted. If you choose to submit **As soon as possible** statistical information will be sent immediately after it is created. This setting is suitable if a permanent Internet connection is available. If **During update** is selected, statistical information will be kept and submitted collectively during the next update.



4.9.3 Submission

In this section, you can choose whether files and statistical information will be submitted by means of ESET Remote Administrator or directly to ESET. If you want to be sure that suspicious files and statistical information are delivered to ESET, select the option **By means of Remote Administrator or directly to ESET**. If this option is selected, files and statistics are submitted by all available means. Submission of suspicious files by means of Remote Administrator submits files and statistics to the remote administration server, which will ensure their subsequent submission to ESET's virus labs. If the option **Directly to ESET** is selected, all suspicious files and statistical information are sent to ESET's virus lab directly from the program.



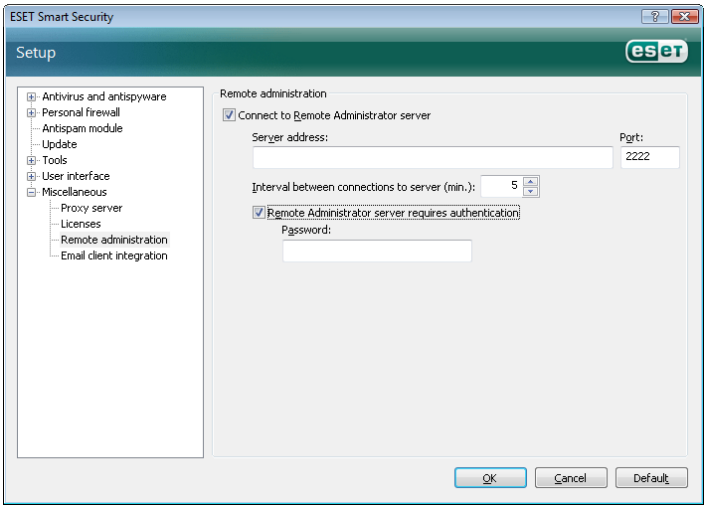
Where there are files pending submission, the **Submit now** button is activated in this setup window. Click this button if you wish to immediately submit files and statistical information.

Select the **Enable logging** check box to enable recording of file and statistical information submission. After each submission of a suspicious file or a piece of statistical information, an entry in the event log is created.

4.10 Remote administration

Remote administration is a powerful tool for maintaining security policy and for obtaining an overview of the overall security management within the network. It is especially useful when applied to larger networks. Remote Administration not only increases the security level, but also provides ease-of-use in the administration of ESET Smart Security on client workstations.

The Remote administration setup options are available from the main ESET Smart Security program window. Click **Setup > Enter the entire advanced setup tree... > Miscellaneous > Remote administration**.



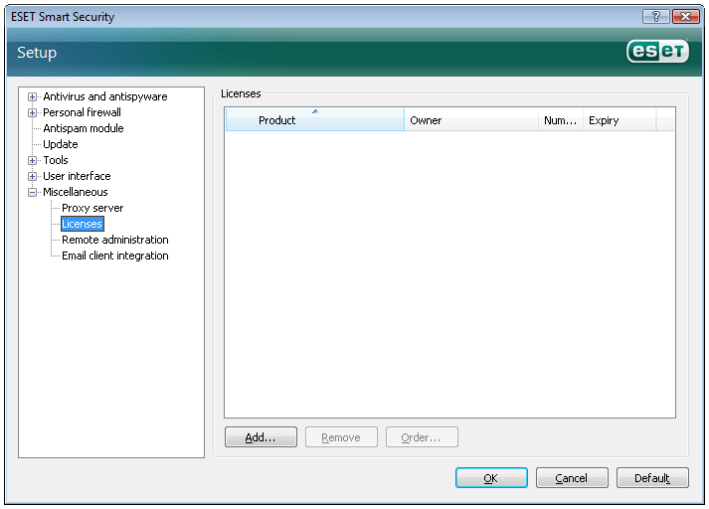
The Setup window allows you to activate the remote administration mode by first selecting the **Connect to Remote Administration server check**. You can then access the other options described below:

- **Server address** – Network address of the server where the remote administration server is installed.
- **Port** – This field contains a predefined server port used for connection. We recommend that you leave the predefined port setting of 2222.
- **Interval between connections to server (min.)** – This designates the frequency with which ESET Smart Security will connect to the ERA server to send out the data. In other words, information is sent at the time intervals defined here. If it is set to 0, information will be submitted every 5 seconds.
- **Remote Administrator requires authentication** – Allows you to enter a password for connecting to the remote administration server, if required.

Click **OK** to confirm changes and apply the settings. ESET Smart Security will use these settings to connect to the remote server.

4.11 License

The **License** branch allows you to manage the license keys for ESET Smart Security and other ESET products such as ESET Remote Administrator, ESET NOD32 for Microsoft Exchange, etc. After purchase, license keys are delivered along with your User name and Password. To **Add/Remove** a license key, click the corresponding button in the license manager window. The license manager is accessible from the Advanced Setup tree under **Miscellaneous > Licenses.**



The license key is a text file containing information about the purchased product: its owner, number of licenses, and the expiry date.

The license manager window allows the user to upload and view the content of a license key using the **Add**... button – the information contained is displayed in the manager. To delete license files from the list, click **Remove**.

If a license key has expired and you are interested in purchasing a renewal, click the **Order... button** – you will be redirected to our online store.

5. Advanced user

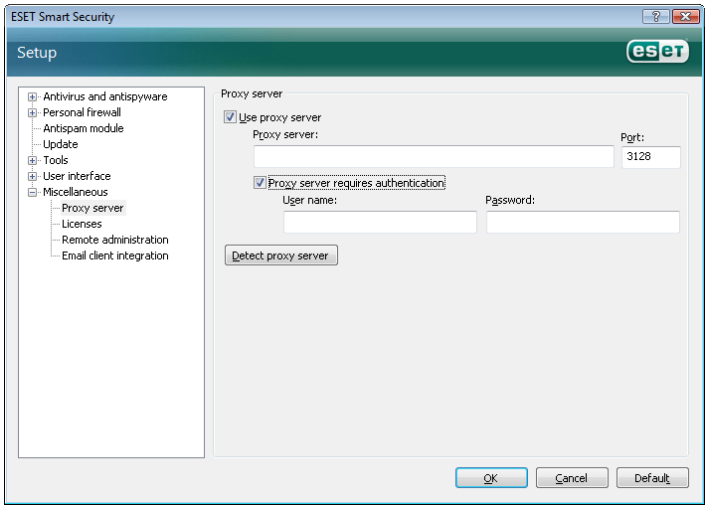
This chapter describes features of ESET Smart Security which may come in handy for more advanced users. Setup options for these features are accessible only in Advanced mode. To switch to Advanced mode, click **Toggle Advanced mode** in the bottom left corner of the main program window or press CTRL + M on your keyboard.

5.1 Proxy server setup

In ESET Smart Security, proxy server setup is available in two different sections within the Advanced Setup tree structure.

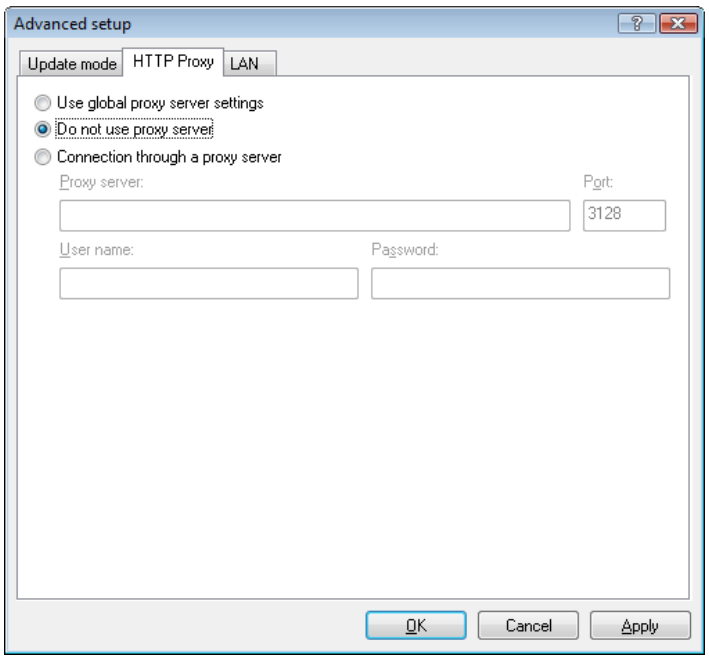
First, proxy server settings can be configured under **Miscellaneous > Proxy server**. Specifying the proxy server at this level defines global proxy server settings for all of ESET Smart Security. Parameters here will be used by all modules requiring connection to the Internet.

To specify proxy server settings for this level, select the **Use proxy server** check box and then enter the address of the proxy server into the **Proxy server:** field, along with the **Port** number of the proxy server.



If communication with the proxy server requires authentication, select the **Proxy server requires authentication** check box and enter a valid **User name** and **Password** into the respective fields. Click the **Detect proxy server** button to automatically detect and insert proxy server settings. The parameters specified in Internet Explorer will be copied. Please note that this feature does not retrieve authentication data (User name and Password), they must be supplied by the user.

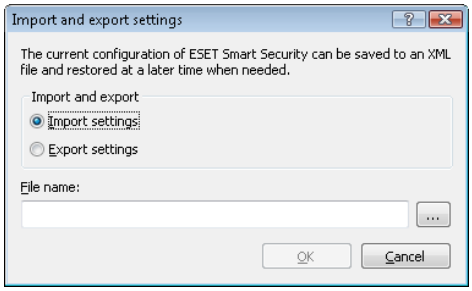
Proxy server settings can also be established within the **Advanced update setup** (**Update** branch of the Advanced Setup tree). This setting applies for the given update profile and is recommended for laptops, as they often receive virus signature updates from different locations. For more information about this setting, see Section 4.4, "Updating the system".



5.2 Export / import settings

Export and import of the current configuration of ESET Smart Security is available in Advanced mode under **Setup**.

Both export and import utilize the .xml file type. Export and import are useful if you need to back up the current configuration of ESET Smart Security in order to be able to use it later (for whatever reason). The export settings option will also be appreciated by those who want to use their favorite configuration of ESET Smart Security on multiple systems - they just need to import their .xml file.


Import and export settings
The current configuration of ESET Smart Security can be saved to an XML file and restored at a later time when needed.
Import and export
Import settings
Export settings
File name:
...
OK
Cancel

5.2.1 Export settings

Export of configuration is very easy. If you want to save the current configuration of ESET Smart Security, click **Setup > Import and export settings...**. Select the **Export settings** option and enter the name of the configuration file. Use the browser to select a location on your computer where you wish to save the configuration file to.

5.2.2 Import settings

The steps for importing a configuration are very similar. Again, select **Import and export settings**, and select the **Import settings** option. Click the **...** button and browse for the configuration file you wish to import.

5.3 Command Line

ESET Smart Security's antivirus module can be launched via the command line – manually (with the "ecls" command) or with a batch ("bat") file.

The following parameters and switches can be used while running the on-demand scanner from the command line:

General options:

– help	show help and quit
– version	show version information and quit
– base-dir = FOLDER	load modules from FOLDER
– quar-dir = FOLDER	quarantine FOLDER
– aind	show activity indicator

Targets:

– files	scan files (default)
– no-files	do not scan files
– boots	scan boot sectors (default)
– no-boots	do not scan boot sectors
– arch	scan archives (default)
– no-arch	do not scan archives
– max-archive-level = LEVEL	maximum archive nesting LEVEL
– scan-timeout = LIMIT maximum. If the scanning of the continue with the	scan archives for LIMIT seconds at scanning time reaches this limit, the archive is stopped and the scan will next file
– max-arch-size=SIZE archives (default 0 =	scan only the first SIZE bytes in unlimited)
– mail	scan email files
– no-mail	do not scan email files
– sfx	scan self-extracting archives
– no-sfx	do not scan self-extracting archives
– rtp	scan runtime packers
– no-rtp	do not scan runtime packers
– exclude = FOLDER	exclude FOLDER from scanning
– subdir	scan subfolders (default)
– no-subdir	do not scan subfolders
– max-subdir-level = LEVEL (default 0	maximum subfolder nesting LEVEL = unlimited)
– symlink	follow symbolic links (default)
– no-symlink	skip symbolic links
– ext-remove = EXTENSIONS	
– ext-exclude = EXTENSIONS colon from scanning	exclude EXTENSIONS delimited by

Methods:

– adware	scan for Adware/Spyware/Riskware
– no-adware Riskware	do not scan for Adware/Spyware/
– unsafe applications	scan for potentially unsafe
– no-unsafe applications	do not scan for potentially unsafe
– unwanted applications	scan for potentially unwanted
– no-unwanted applications	do not scan for potentially unwanted
– pattern	use signatures
– no-pattern	do not use signatures
– heur	enable heuristics
– no-heur	disable heuristics
– adv-heur	enable Advanced heuristics
– no-adv-heur	disable Advanced heuristics

Cleaning:

– action = ACTION Available actions: none, clean, prompt	perform ACTION on infected objects.
– quarantine (supplements ACTION)	copy infected files to Quarantine
– no-quarantine Quarantine	do not copy infected files to

Logs:

– log-file=FILE	log output to FILE
– log-rewrite	overwrite output file (default – append)
– log-all	log also clean files
– no-log-all	do not log clean files (default)

The possible exit codes of the scan:

0 – no threat found
1 – threat found but not cleaned
10 – some infected files remained
101 – archive error
102 – access error
103 – internal error

NOTE:
Exit codes greater than 100 mean that the file was not scanned and thus can be infected.

6. Glossary

6.1 Types of infiltrations

An Infiltration is a piece of malicious software trying to enter and/or damage a user's computer.

6.1.1 Viruses

A computer virus is an infiltration which corrupts existing files on your computer. Viruses are named as such after biological viruses, as they use similar techniques to spread from one computer to another.

Computer viruses attack mainly executable files and documents. To replicate, a virus attaches its "body" to the end of a target file. In short, this is how a computer virus works: after execution of the infected file, the virus activates itself (before the original application) and performs its predefined task. Only after that is the original application allowed to run. A virus cannot infect a computer unless a user (either accidentally or deliberately) runs or opens the malicious program by him/herself.

Computer viruses can range in activity and severity. Some of them are extremely dangerous because of their ability to purposely delete files from a hard drive. On the other hand, some viruses cause no real damage – they only serve to annoy the user and demonstrate the technical skills of their authors.

It is important to note that viruses are (when compared to trojans or spyware) gradually becoming more of a rarity, since they are not commercially enticing for authors of malicious software. Also, the term "virus" is often incorrectly used to cover all types of infiltrations. At present, this is gradually being overcome and the new, more accurate term "malware" (malicious software) is used.

If your computer is infected with a virus, it is necessary to restore infected files to their original state – i.e. to clean them by using an antivirus program.

Examples of viruses are: OneHalf, Tenga, and Yankee Doodle.

6.1.2 Worms

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The basic difference between a virus and a worm is that worms have the ability to replicate and travel by themselves. They are not dependent on host files (or boot sectors).

Worms proliferate by means of email or network packets. In this regard, worms can be categorized two ways:

- **Email** – distributing themselves to email addresses found in a user's contact list and
- **Network** – exploiting security vulnerabilities in various applications.

Worms are therefore much more viable than computer viruses. Due to the wide availability of the Internet, they can spread across the globe within hours of their release – in some cases, even in minutes. This ability to replicate independently and rapidly makes them more dangerous than other types of malware, such as viruses.

A worm activated in a system can cause a number of inconveniences: It can delete files, degrade system performance, or even deactivate some programs. The nature of a computer worm qualifies it as a "means of transport" for other types of infiltrations.

If your computer is infected with a computer worm, we recommend that you delete infected files, because they likely contain malicious code.

Examples of well-known worms are: Lovsan/Blaster, Stration/Warezov, Bagle, and Netsky.

6.1.3 Trojan horses

Historically, computer trojan horses have been defined as a class of infiltrations which attempt to present themselves as useful programs, thus tricking users into letting them run. But it is important to note that this was true for trojan horses in the past–today, there is no longer a need for them to disguise themselves. Their sole purpose is to infiltrate as easily as possible and accomplish their malicious goals. "Trojan horse" has become a very general term describing any infiltration not falling under any specific class of infiltration.

Since this is a very broad category, it is often divided into many subcategories. The most widely known are:

- downloader – a malicious program with the ability to download other infiltrations from the Internet.
- dropper – a type of trojan horse designed to drop other types of malware onto compromised computers.
- backdoor – an application which communicates with remote attackers, allowing them to gain access to a system and to take control of it.
- keylogger – (keystroke logger) – a program which records each keystroke that a user types and sends the information to remote attackers.
- dialer – dialers are programs designed to connect to premium-rate numbers. It is almost impossible for a user to notice that a new connection was created. Dialers can only cause damage to users with dial-up modems, which are no longer regularly used.

Trojan horses usually take the form of executable files with the extension .exe. If a file on your computer is detected as a trojan horse, it is advisable to delete it, since it most likely contains malicious code.

Examples of well-known trojans are: NetBus, Trojandownloader. Small.ZL, Slapper

6.1.4 Rootkits

Rootkits are malicious programs that grant Internet attackers unlimited access to a system, while concealing their presence. Rootkits, after accessing a system (usually exploiting a system vulnerability), use functions in the operating system to avoid detection by antivirus software: they conceal processes, files and Windows registry data. For this reason, it is almost impossible to detect them using ordinary testing techniques.

When it comes to rootkit prevention, remember that there are two levels of detection:

1. When they try to access a system. They are still not present, and are therefore inactive. Most antivirus systems are able to eliminate rootkits at this level (assuming that they actually detect such files as being infected).
2. When they are hidden from the usual testing. Users of the ESET antivirus system have the advantage of Anti-Stealth technology, which is also able to detect and eliminate active rootkits.

6.1.5 Adware

Adware is a short for advertising-supported software. Programs displaying advertising material fall under this category. Adware applications often automatically open a new pop-up window containing advertisements in an Internet browser, or change the browser's home page. Adware is often bundled with freeware programs, allowing their creators to cover development costs of their (usually useful) applications.

Adware itself is not dangerous – users will only be bothered with advertisements. Its danger lies in the fact that adware may also

perform tracking functions (as spyware also does).

If you decide to use a freeware product, please pay particular attention to the installation program. The installer will most likely notify you of the installation of an extra adware program. Often you will be allowed to cancel it and install the program without adware. On the other hand, some programs will not install without adware, or their functionality will be limited. This means that adware may often access the system in a "legal" way, because users have agreed to it. In this case, it is better to be safe than sorry.

If there is a file detected as adware on your computer, it is advised to delete it, since it most likely contains malicious code.

6.1.6 Spyware

This category covers all applications which send private information without user consent/awareness. They use tracking functions to send various statistical data such as a list of visited web sites, email addresses from the user's contact list, or a list of recorded keystrokes.

The authors of spyware claim that these techniques aim to find out more about users' needs and interests and allow better-targeted advertisement. The problem is that there is no clear distinction between useful and malicious applications and no one can be sure that the retrieved information will not be misused. The data obtained by spyware applications may contain security codes, PINs, bank account numbers, etc. Spyware is often bundled with free versions of a program by its author in order to generate revenue or to offer an incentive for purchasing the software. Often, users are informed of the presence of spyware during a program's installation to give them an incentive to upgrade to a paid version without it.

Examples of well-known freeware products which come bundled with spyware are client applications of P2P (peer-to-peer) networks. Spyfalcon or Spy Sheriff (and many more) belong to a specific spyware subcategory – they appear to be antispyware programs, but in fact they are spyware programs themselves.

If there is a file detected as spyware on your computer, it is advisable to delete it, since it most likely contains malicious code.

6.1.7 Potentially unsafe applications

There are many legitimate programs which serve to simplify the administration of networked computers. However, in the wrong hands, they may be misused for malicious purposes. This is why ESET has created this special category. Our clients now have the option to choose whether the antivirus system should or should not detect such threats.

"Potentially unsafe applications" is the classification used for commercial, legitimate software. This classification includes programs such as remote access tools, password-cracking applications, and keyloggers (a program recording each keystroke a user types).

If you find that there is a potentially unsafe application present and running on your computer (and you did not install it), please consult your network administrator or remove the application.

6.1.8 Potentially unwanted applications

Potentially unwanted applications are not necessarily intended to be malicious, but may affect the performance of your computer in a negative way. Such applications usually require consent for installation. If they are present on your computer, your system behaves differently (compared to the state before their installation). The most significant changes are:

- new windows you haven't seen previously are opened
- activation and running of hidden processes
- increased usage of system resources
- changes in search results
- application communicates with remote servers

6.2 Types of remote attacks

There are many special techniques which allow attackers to compromise remote systems. These are divided into several categories.

6.2.1 DoS attacks

DoS, or Denial of Service, is an attempt to make a computer or network unavailable for its intended users. The communication between afflicted users is obstructed and can no longer continue in a functional way. Computers exposed to DoS attacks usually need to be restarted in order to work properly.

In most cases, the targets are web servers and the aim is to make them unavailable for users for a certain period of time.

6.2.2 DNS Poisoning

Through the DNS (Domain Name Server) poisoning method, hackers can trick the DNS server of any computer into believing that the fake data they supplied is legitimate and authentic. The fake information is cached for a certain period of time, allowing attackers to rewrite DNS replies of IP addresses. As a result, users trying to access Internet web sites will download computer viruses or worms instead of their original content.

6.2.3 Worm attacks

A computer worm is a program containing malicious code that attacks host computers and spreads via a network. The network worms exploit security vulnerabilities in various applications. Due to the availability of the Internet, they can spread all over the world within a few hours of their release. In some cases, even in minutes.

Most worm attacks (Sasser, SqlSlammer) can be avoided by using default security settings in the firewall, or by blocking unprotected and unused ports. Also, it is essential that your operating system is updated with the most recent security patches.

6.2.4 Port scanning

Port scanning controls whether there are open computer ports on a network host. A port scanner is software designed to find such ports.

A computer port is a virtual point which handles incoming and outgoing data – this is crucial from a security point of view. In a large network, the information gathered by port scanners may help to identify potential vulnerabilities. Such use is legitimate.

Still, port scanning is often used by hackers attempting to compromise security. Their first step is to send packets to each port. Depending on the response type, it is possible to determine which ports are in use. The scanning itself causes no damage, but be aware that this activity can reveal potential vulnerabilities and allow attackers to take control of remote computers.

Network administrators are advised to block all unused ports and protect those that are in use from unauthorized access.

6.2.5 TCP desynchronization

TCP desynchronization is a technique used in TCP Hijacking attacks. It is triggered by a process in which the sequential number in incoming packets differs from the expected sequential number. The packets with an unexpected sequential number are dismissed (or saved in the buffer storage, if they are present in the current communication window).

In the state of desynchronization, both communication endpoints

dismiss received packets. This is the point when remote attackers are able to infiltrate and supply packets with a correct sequential number. The attackers can even manipulate the communication with their commands, or modify it some other way.

TCP Hijacking attacks aim to interrupt server-client, or peer-to-peer communications. Many attacks can be avoided by using authentication for each TCP segment. It is also advised to use the recommended configurations for your network devices.

6.2.6 SMB Relay

SMBRelay and SMBRelay2 are special programs able to carry out an attack against remote computers. The programs take advantage of the Server Message Block file sharing protocol, which is layered onto NetBIOS. If a user shares any folder or directory within the LAN, he or she most likely uses this file sharing protocol.

Within the local network communication, password hashes are exchanged.

SMBRelay receives a connection on UDP port 139 and 445, relays the packets exchanged by the client and server, and modifies them. After connecting and authenticating, the client is disconnected. SMBRelay creates a new virtual IP address. The new address can be accessed using the command "net use \\192.168.1.1". The address can then be used by any of the Windows networking functions. SMBRelay relays SMB protocol communication except for negotiation and authentication. Remote attackers can use the IP address, as long as the client computer is connected.

SMBRelay2 works on the same principle as SMBRelay, except it uses NetBIOS names rather than IP addresses. Both of them can carry out "man-in-the-middle" attacks. These attacks allow remote attackers to read, insert and modify messages exchanged between two communication endpoints without being noticed. Computers exposed to such attacks often stop responding or unexpectedly restart.

To avoid attacks, we recommend that you use authentication passwords or keys.

6.2.7 ICMP attacks

The ICMP (Internet Control Message Protocol) is a popular and widely-used Internet protocol. It is used primarily by networked computers to send various error messages.

Remote attackers attempt to exploit the weaknesses of the ICMP protocol. The ICMP protocol is designed for one-way communication requiring no authentication. This enables remote attackers to trigger so-called DoS (Denial of Service) attacks, or attacks which give unauthorized individuals access to incoming and outgoing packets.

Typical examples of an ICMP attack are ping flood, ICMP_ECHO flood and smurf attack. Computers exposed to the ICMP attack are significantly slower (this applies to all applications using the Internet) and have problems connecting to the Internet.

6.3 Email

Email, or electronic mail, is a modern form of communication with many advantages. It is flexible, fast and direct. Email played a crucial role in the proliferation of the Internet in the early 1990's.

Unfortunately, with their high level of anonymity, email and the Internet leave room for illegal activities such as spamming. Broadly categorized, spam includes unsolicited advertisements, hoaxes and proliferation of malicious software – malware. The inconvenience and danger to the user is increased by the fact that the costs of sending are next to zero, and authors of spam have many tools and sources available to acquire new email addresses. In addition, the volume and variety of spam makes it very difficult to regulate. The longer you use your email address, the higher the possibility of it ending up in a spam engine database. Some hints for prevention:

- If possible, don't publish your email address on the Internet
- Only give your email address to trusted individuals
- If possible, don't use common aliases – with more complicated aliases, the probability of tracking is lower
- Don't reply to spam that has already arrived in your inbox
- Be careful when filling out Internet forms – be especially aware of checkboxes such as "Yes, I want to receive information about... in my inbox."
- Use "specialized" email addresses – e.g. one for your work, one for communication with your friends, etc.
- From time to time, change your email address
- Use an Antispam solution

6.3.1 Advertisements

Internet advertising is one of the most rapidly growing forms of advertising. Email advertising uses email as a means of contact. Its main marketing advantages are zero costs, high level of directness and effectiveness; what's more, messages are delivered almost immediately. Many companies use email marketing tools to effectively communicate with their current and prospective customers.

This means of advertising is legitimate, since the user may be interested in receiving commercial information about some products. But the fact is that many companies send unsolicited bulk commercial messages. In such cases, email advertising crosses the line and becomes spam.

The amount of unsolicited commercial e-mail has become a real problem, since it shows no signs of abating. Authors of unsolicited email naturally try to masquerade spam as legitimate messages. On the other hand, legitimate advertising in large quantities may cause negative reactions.

6.3.2 Hoaxes

A hoax is a message spread across the Internet. Usually it is sent via email and sometimes via communication tools like ICQ and Skype. The message itself is often a joke or Urban Legend.

Computer Virus hoaxes try to generate fear, uncertainty and doubt (FUD) in the recipients, bringing them to believe that there is an "undetectable virus" deleting files and retrieving passwords, or performing some other harmful activity on their system.

Some hoaxes are meant to cause emotional embarrassment to others. Recipients are usually asked to forward such messages to all their contacts, which perpetuates the life-cycle of the hoax. There are mobile phone hoaxes, pleas for help, people offering to send you money from abroad, etc. In most cases it is impossible to track down the intent of the creator.

In principle, if you see a message prompting you to forward it to everyone you know, it may very well be a hoax. There are many specialized web sites on the Internet which can verify whether an email is legitimate or not. Before forwarding, perform an Internet search on any message you suspect of being a hoax.

6.3.3 Phishing

The term phishing defines a criminal activity which uses techniques of social engineering (manipulating users in order to obtain confidential information). Its aim is to gain access to sensitive data such as bank account numbers, PIN codes, etc.

Access is usually achieved by sending email masquerading as a trustworthy person or business (financial institution, insurance company). The email can look very genuine, and will contain graphics and content which may have originally come from the source that it is impersonating. You will be asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers or user names and passwords. All such data, if submitted, can easily be stolen and misused.

It should be noted that banks, insurance companies, and other legitimate companies will never request user names and passwords in an unsolicited email.

6.3.4 Recognizing spam scams

Generally, there are a few indicators which can help you identify spam (unsolicited emails) in your mailbox. If a message fulfils at least some of the following criteria, it is most likely a spam message.

- sender address does not belong to someone on your contact list
- you are offered a large sum of money, but you have to provide a small sum first
- you are asked to enter, under various pretenses (data verification, financial operations), some of your personal data – bank account numbers, user names and passwords, etc.
- it is written in a foreign language
- you are asked to buy a product you are not interested in. If you decide to purchase anyway, please verify that the message sender is a reliable vendor (consult the original product manufacturer).
- some of the words are misspelled in an attempt to trick your spam filter. For example „vaigra" instead of "viagra", etc.

6.3.4.1 Rules

In the context of Antispam solutions and email clients, rules are tools for manipulating email functions. They consist of two logical parts:

1. condition (for example, an incoming message from a certain address)
2. action (for example, deletion of the message, moving it to a specified folder).

The number and combination of rules varies with the Antispam solution. These rules serve as measures against spam (unsolicited email). Typical examples:

- 1. condition: An incoming email contains some of the words typically seen in spam messages
  2. action: Delete the message
- 1. condition: An incoming email contains an attachment with a .exe extension
  2. action: Delete the attachment and deliver the message to the mailbox
- 1. condition: An incoming message arrives from your employer
  2. action: Move the message to the „Work" folder.

We recommend that you use a combination of rules in Antispam programs in order to facilitate administration and to more effectively filter spam (unsolicited email).

6.3.4.1 Bayesian filter

Bayesian spam filtering is a very effective form of email filtering used by almost all Antispam products. It is able to identify unsolicited email with a high degree of accuracy. The Bayesian filter can work on a per-user basis.

The functionality is based on the following principle: The learning process takes place in the first phase. The user manually marks a sufficient number of messages as legitimate messages or as spam (normally 200/200). The filter analyzes both categories and learns, for example, that spam usually contains words "rolex" or "viagra", and legitimate messages are sent by family members or from addresses in the user's contact list. Provided that a greater number of messages was processed, the Bayesian filter is able to assign a certain "spam index" to each message and thus decide on whether it is spam or not.

The main advantage is its flexibility. If a user is, say, a biologist, all incoming emails concerning biology or a relative fields of study will generally receive a lower probability index. If a message includes words that would otherwise qualify it as being unsolicited, but it is sent by someone from a contact list, it will be marked as legitimate, because senders from a contact list decrease overall spam probability.

6.3.4.2 Whitelist

In general, a whitelist is a list of items or persons who are accepted, or have been granted access permission. The term „email whitelist" defines a list of contacts from whom the user wishes to receive messages. Such whitelists are based on keywords searched for in email addresses, domain names, or IP addresses.

If a whitelist works in „exclusivity mode", then messages from any other address, domain, or IP address will not be received. On the other hand, if it is not exclusive, such messages will not be deleted, but filtered in some other way.

A whitelist is based on the opposite principle to that of a blacklist. Whitelists are relatively easy to maintain, more so than blacklists. We recommend that you use both the Whitelist and Blacklist to filter spam more effectively.

6.3.4.3 Blacklist

Generally, a blacklist is a list of unaccepted or forbidden items or persons. In the virtual world, it is a technique enabling acceptance of messages from all users not present on such a list.

There are two types of blacklist. It is possible for users to create their own blacklist in their Antispam program. On the other hand, many professional, regularly updated blacklists created by specialized institutions can be found on the Internet.

Blacklist is based on the opposite principle to that of whitelist. It is essential to use blacklists to successfully block spam, but they are very difficult to maintain, since new items to be blocked appear every day. We recommended that you use both the Whitelist and Blacklist to filter out spam more effectively.

6.3.4.5 The server-side control

The server-side control is a technique for identifying mass spam email based on the number of received messages and the reactions of users. Each message leaves a unique digital „footprint" on the server based on the content of the message. In fact, it is a unique ID number which tells nothing about the content of the e-mail. Two identical messages will have identical footprints, while different messages will have different footprints.

If a message is marked as spam, its footprint is sent to the server. If the server receives more identical footprints (corresponding to a certain spam message), the footprint is stored at the spam footprints database. When scanning incoming messages, the program sends the footprints of the messages to the server. The server returns information on which footprints correspond to messages already marked by users as spam.